ACADEMIA MILITAR

A Cibersegurança e as Estruturas Críticas: A GNR

Ciberguarda, o Futuro

Autor: Aspirante de Infantaria da GNR Filipe Reina Fernandes

Orientador: TCOR TMS Paulo Fernando V. Nunes

Co-Orientador: TEN TIE Filipe Tavares Rodrigues

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, Agosto de 2013

ACADEMIA MILITAR

A Cibersegurança e as Estruturas Críticas: A GNR

Ciberguarda, o Futuro

Autor: Aspirante de Infantaria da GNR Filipe Reina Fernandes

Orientador: TCOR TMS Paulo Fernando V. Nunes

Co-Orientador: TEN TIE Filipe Tavares Rodrigues

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, Agosto de 2013

Dedicatória

À minha família.

Agradecimentos

O presente trabalho é produto de um enorme conjunto de contributos e empenho de várias pessoas, sem as quais não seria possível a realização do mesmo. Por esse motivo, manifesto o meu profundo agradecimento ao meu orientador, o Sr. Tenente Coronel Paulo Fernandes Viegas Nunes, pela sublime dedicação que demonstrou e pela sua infatigável disponibilidade, constituindo-se sobejamente como uma referência a seguir no futuro.

Agradeço também ao Sr. Tenente João Filipe Tavares Rodrigues, meu co-orientador, por todo o apoio, colaboração e interesse que demostrou desde o início da realização deste trabalho., pelo seu contributo, as suas críticas e pela forma como se disponibilizou em facultar-me todas as informações e estabelecer todos os contactos necessários dentro da Instituição tendo em vista a realização deste trabalho, foram cruciais para a realização do mesmo.

Agradeço aos Senhores Oficiais da Guarda Nacional Republicana que se seguem, a forma como se prontificaram e se mostraram disponíveis, desde logo, para me concederem entrevistas fundamentais para o desenvolvimento e, posteriores conclusões do trabalho.

Sr. Major Bessa pela partilha de experiências e de informações que tanto contribuíram para a compreensão deste fenómeno.

Sr. Capitão Raposo pela sua disponibilidade e por me transmitir alguns dos seus conhecimentos e experiências numa área tão sensível como esta da gestão e segurança dos nossos sistemas informáticos.

Sr. Major Santos pela forma como se disponibilizou para transmitir os seus conhecimentos nesta área, mas sobretudo por partilhar comigo a sua visão do futuro da GNR relativamente à Cibersegurança.

Sr. Major Pimentel pela sua explicação mais pragmática dos contornos da Cibersegurança.

Sr. Coronel Nunes pela explicação das competências da GNR relacionadas com a Cibersegurança e Cibercrime.

Estendo os agradecimentos ao meu Curso, por todos os bons momentos que me proporcionaram e que com certeza serão eternos.

Agradeço também à minha família, em especial aos meus pais e irmão, por todo o apoio e compreensão.

Por último, mas não menos importante, agradeço a todos aqueles cujo nome não se encontra aqui presente mas que por diversas formas, cedendo dados, informações, opiniões, ou através da sua experiência pessoal e profissional, contribuíram para a realização deste trabalho. A todos Vós o meu obrigado.

Resumo

Nas últimas duas décadas, a Internet e o ciberespaço tiveram um impacto enorme em todos os sectores da sociedade, relacionando-se com todos os aspectos da vivência na era da Informação. Fazendo uma análise abrangente, neste momento, a nossa sociedade e o Ciberespaço são duas realidades indissociáveis.

A nossa vida diária, os direitos fundamentais, as interacções sociais e as economias dependem continuamente do funcionamento das tecnologias da informação e comunicação.

Com a crescente importância das Tecnologias da Informação e Comunicação em todas as esferas da sociedade, a questão da Cibersegurança assumiu uma dimensão estratégica em especial, na Segurança e Defesa Nacional. De acordo com a sua natureza e capacidade disruptiva os ciberataques podem pôr em risco as Infra-Estruturas Críticas nacionais.

A protecção do Ciberespaço acarreta novos e grandes desafios e há muito por fazer, quer no plano internacional, quer nacional. Com diferentes níveis de responsabilidade, tanto a indústria, como os cidadãos e os Estados, são partes interessadas na cibersegurança como garantia dos bens jurídicos fundamentais e do regular funcionamento das instituições.

Neste contexto, a atribuição de responsabilidades e competências no âmbito do Ciberespaço, entendido como uma extensão virtual do mundo real em que habitamos, deverá obedecer à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa do Estado.

Face ao desenvolvimento da cibercriminalidade e ao crescente número de incidentes e intrusões a sistemas de vários órgãos e instituições nacionais, as Forças de Segurança têm que proteger os seus sistemas de informação e terão ainda de prosseguir as novas políticas de Cibersegurança Internacionais e Nacionais.

Relativamente à metodologia e a fim de alcançar os objectivos definidos para a investigação, principiou-se por efectuar um levantamento do Estado da Arte, recorrendo, para o efeito, à pesquisa e à análise documental em obras ligadas à temática.

Simultaneamente, aplicando o método inquisitivo, procedeu-se à realização de entrevistas semi-directivas, às principais entidades que detêm o conhecimento crítico nesta área de estudo e também os responsáveis pelas diversas estruturas alvo de estudo e análise, correspondendo estes capítulos à fase analítica.

No decorrer da elaboração do trabalho foi constatado que a Cibersegurança será uma das principais preocupações dos Estados neste século, em particular no que diz respeito à segurança das Infra-Estruturas Críticas de Informação. Ao longo do trabalho foi possível conhecer a vertente da Cibersegurança da Guarda e pelos testemunhos recolhidos e análise da legislação é também possível prever que será exigido à GNR adaptar-se a esta nova realidade.

Esta adaptação deve ser orientada por seis objectivos, sendo eles: a Investigação e Desenvolvimento, Normalização e Certificação, Formação e Consciencialização, Alerta e Resposta a Incidentes, Combate ao Cibercrime e Protecção de Infra-Estruturas Críticas.

Um grande contributo para a cibersegurança do nosso país, seria o desenvolvimento de "Programas Especiais de Polícia" ligados ao *Cyber-Policing*, tendo em vista a consciencialização dos cidadãos e de outros sectores público-privados sobre as diversas formas que existem para minimizar os seus efeitos. E desenvolver ainda as valências de *business continuity* e *disaster recovery*.

Palavras-Chave: Cibersegurança, Ciberespaço, Ciberameaças, Guarda Nacional Republicana.

Abstract

In the last two decades, the Internet and Cyberspace had a huge impact in all sectors of society, and are related to all aspects of living in the age of information. Making an introspective analysis, right now, our society and Cyberspace are inseparable realities.

In our daily life, the fundamental rights, social interactions and economies depend on the continuous function of the Information and Communication Technologies.

With the growing importance of Information and Communication Technologies in all spheres of society, the issue of Cybersecurity assumed a strategic dimension in particular in the National Security and Defense Strategies. Taking into account its nature and capacity, disruptive cyber-attacks can jeopardize Critical National Infrastructures.

The protection of cyberspace brings new challenges and much work to be done, either Nationally and Internationally. With different levels of responsibility, industry, citizens and states are stakeholders in cybersecurity as a guarantor of fundamental legal rights.

In this context, the allocation of responsibilities and powers under Cyberspace, conceptualized as a virtual extension of the real world we inhabit, it should follow the same logic and principles which characterize the security and defense of the state.

Given the development of Cybercrime and the growing number of incidents and intrusions to various Organs and Systems of National Institutions, Security Forces in addition to having to protect their information systems and continue with the existing National and International Cybersecurity policies.

In order to achieve the objectives set for the research, began to conduct a survey on the state of the art, using for this purpose, to research and document analysis in works related to the theme.

Simultaneously, we proceeded to interviews, applying the inquisitive method, through semi-directive questioning, the main entities that hold critical knowledge in this area of study and also those responsible for the different structures that are the focus of the study and analysis, corresponding to the chapters of the analytical phase.

During the research we found that Cybersecurity will be one of the main concerns in this century, specially the security Infrastructure of Critical Information. During this work it was possible to understand GNR role in Cybersecurity and the testimonies collected and analysis of the legislation indicate that GNR will be required to adapt to this new reality.

This adaptation should be driven in six objectives, namely: Research and Development, Standardization and Certification, Training and Awareness, Alert and Incident Response, Cybercrime Fight and Protection of Critical Infrastructure.

A major contribution to the Cybersecurity of our country would be the development of "Special Police Programs" related to Cyber-Policing, with the intent to raising awareness of citizens and other public-private entities about the various ways that exist to minimize their effects. Also develop tools and capabilities of *business continuity* e *disaster recovery*.

Key Words: Cibersecurity, Ciberespace, Ciberthreats, Republican National Guard

Índice

Índice de Figuras

Índice de Quadros

Lista de Siglas

AM – Academia Militar

AMA - Agência para a Modernização Administrativa

ANS - Autoridade Nacional de Segurança

ARPANET - *Advanced Resarch Project Agency Network*

CEGER - O Centro de Gestão da Rede Informática do Governo

CERT.PT - *Computer Emergency Response Team* de Portugal

CNC - Centro Nacional de Cibersegurança

CNPCE - Conselho Nacional de Planeamento Civil de Emergência

CNPCE - O Conselho Nacional de Planeamento Civil de Emergência

CP- Código Penal

CPP – Código do Processo Penal

CSIRT- *Computer Security Incident Response Team*

DCSI - Direcção de Comunicações e Sistemas de Informação

DI - Direcção de Informações

DIC - Direcção de Investigação Criminal

ENISA - *European Network and Information Security Agency*

EU – União Europeia

FCCN - Fundação para a Computação Científica Nacional

FSS – Forças e Serviços de Segurança

GNR – Guarda Nacional Republicana

GNS - Gabinete Nacional de Segurança

ICP-ANACOM - Autoridade Nacional de Comunicações

LC - Lei do Cibercrime

LOIC - Lei de Organização da Investigação Criminal

NEP – Norma de Execução Permanente

OCDE – Organização para a Cooperação e Desenvolvimento Económico

ONU – Organização das Nações Unidas

OPC – Órgão de Polícia Criminal

OTAN – Organização do Tratado do Atlântico Norte

PCSD - Política Comum de Segurança e Defesa

PJ - Polícia Judiciária

PSP – Polícia de Segurança Pública

RCFTIA - Relatório Científico Final do Trabalho de Investigação Aplicada

RNSI – Rede Nacional de Segurança Interna

SCEE - Sistema de Certificação Electrónica do Estado

SIRP - O Sistema de Informações da República Portuguesa

SIS - Serviço de informações e Segurança

SSI - Sistema de Segurança Interna

TI- Tecnologia da informação

TIC Tecnologias da Informação e Comunicação

UMIC – Agência para a Sociedade do Conhecimento

"*Those who attempt to predict the future run the risk of being wrong. But those who overlook the importance of conducting a prospective analysis adopt a passive attitude that weakens them against the dictatorship of events. Anticipating societal changes prepares us to weather the storm".*

"Aqueles que tentam prever o futuro, correm o risco de se enganar. Mas aqueles que ignoram a importância da condução de uma análise prospectiva, adoptam uma atitude passiva que os deixa vulneráveis perante as imprevisibilidades dos acontecimentos. Antecipar as mudanças sociais prepara-nos para sobrevivermos pela passagem da tempestade".

General do Exército Marc Watin-Augouard
Inspector Geral das Forcas Armadas Francesas

Capítulo 1
Introdução

1.1. Enquadramento da investigação

O presente Relatório Científico Final do Trabalho de Investigação Aplicada (RCFTIA), subordinado ao tema "A Cibersegurança e as Estruturas Críticas: A GNR", surge no âmbito do Tirocínio Para Oficiais da Guarda Nacional Republicana sendo um dos elementos de base para o aproveitamento do curso.

Este trabalho visa a aplicação de competências adquiridas e em simultâneo, o desenvolvimento da capacidade de compreensão nos domínios da segurança, estudando um assunto de reconhecido interesse para a GNR, neste caso, estudar e avaliar os principais desafios, o impacto previsto e as implicações para a actividade operacional da GNR, decorrentes do aumento das ciberameaças em geral e da cibercriminalidade em particular. Sendo que, presentemente, todos os Oficiais que vão ingressar nos quadros permanentes da GNR são formados na Academia Militar. Integrado na nova estrutura curricular do curso de formação de Oficiais e destinado à aquisição do grau académico de Mestre, em *Ciências Militares* na especialidade de *Segurança* da GNR, emerge deste modo o presente RCFTIA. Pelo momento em que surge, este representa o culminar de toda uma formação que decorreu ao longo de cinco anos e revela-se uma excelente oportunidade para aprofundar e consolidar os conhecimentos até aí adquiridos. Na sua realização procura-se ainda desenvolver as competências de investigação no âmbito das *Ciências Sociais* e colocar em prática a metodologia inerente a um trabalho científico desta natureza. No humilde intuito de dar um contributo para o corpo de conhecimento existente acerca da GNR, optou-se por desenvolver uma temática que com este estivesse ligado e para a qual se afigurasse de relevante interesse institucional e operacional.

1.2. Importância da investigação e justificação da sua escolha

Com a crescente importância das Tecnologias da Informação e Comunicação (TIC) em todas as esferas da sociedade, em especial, a Segurança e Defesa Nacional, a questão da Cibersegurança assumiu uma dimensão estratégica. De acordo com a sua natureza e capacidade disruptiva, os ciberataques podem por em risco as Infra-Estruturas críticas nacionais.

A protecção do Ciberespaço acarreta novos e grandes desafios e muito há por fazer, quer no plano internacional, quer nacional. Com diferentes níveis de responsabilidade, tanto a indústria, como os cidadãos, como os Estados são partes interessadas na cibersegurança como garante dos bens jurídicos fundamentais.

Neste contexto, a atribuição de responsabilidades e competências no âmbito do Ciberespaço, entendido como uma extensão virtual do mundo real em que habitamos, deverá obedecer à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa do Estado. Obedecendo aos mesmos princípios legais enformadores, as Forças de Segurança serão responsáveis pela Cibersegurança e combate à cibercriminalidade assim como as Forças Armadas devem ser vistas como o corpo social responsável pela Ciberdefesa do País.

Face ao desenvolvimento da cibercriminalidade e ao crescente número de incidentes e intrusões a sistemas de vários órgãos e instituições Nacionais, as Forças de Segurança para além de terem que proteger os seus sistemas de informação terão de prosseguir as novas políticas de Cibersegurança Internacionais e Nacionais.

1.3. Definição de Objectivos

Com a elaboração deste trabalho pretende-se estudar e avaliar os principais desafios, o impacto previsto e as implicações para a actividade operacional da GNR, decorrentes do aumento das Ciberameaças, em geral e da cibercriminalidade, em particular.

É ainda objectivo deste trabalho entender o modelo de articulação e de cooperação entre as entidades que participam na cibersegurança e ciberdefesa nacionais.

Pretende-se também analisar o volume de ameaças e ataques às nossas redes e Infra-Estruturas Críticas.

A fim de prosseguir os objectivos de investigação, como questão central e ponto de partida para o trabalho, foi apresentado o seguinte problema:

1.3.1. Questão central

"Face à necessidade de garantir a Cibersegurança das estruturas críticas nacionais, quais as principais implicações, impacto previsto e que desafios operacionais se colocam à actividade da GNR?

Com vista a concretizar parâmetros de resposta à questão central foram levantadas as seguintes questões derivadas.

1.3.2. Questões derivadas

QD 1:O que é o Ciberespaço e que desafios coloca às modernas sociedades e ao ambiente de segurança?

QD 2:O que é e como é possível garantir a Cibersegurança das Estruturas Críticas Nacionais?

QD 3: Qual é o espectro da ameaça no Ciberespaço e quais os principais desafios se colocam às Forças de Segurança e à GNR em particular?

QD 4: Qual o impacto das Ciberameaças na actividade operacional da GNR?

QD 5: Que alterações serão necessários realizar na GNR para garantir uma maior eficácia, no desempenho da sua missão em prol da Cibersegurança das Estruturas críticas?

1.3.3. Hipóteses

H1 – O Ciberespaço tem cada vez mais importância na actualidade.

H2 – O Ciberespaço acarreta responsabilidades de segurança para o Estado e as suas Forças de Segurança.

H3 – Portugal tem uma Estratégia de Cibersegurança capaz de garantir a segurança das Estruturas Críticas.

H4 – As Infra-Estruturas Críticas da GNR são seguras.

H5 – A GNR mantêm o seu nível de Operacionalidade no caso de ser alvo de um ataque às suas Infra-Estruturas Críticas.

H6 – Os Modelos de Actuação da GNR satisfazem as necessidades de Cibersegurança da sua competência.

1.4. Metodologia

O método científico, característico de um RCFTIA em Ciências Sociais, encontra-se regulado pela NEP 520/30JUN11/AM o qual padroniza a sua concepção.

Podemos definir investigação como "o diagnóstico das necessidades de informação e selecção das variáveis relevantes sobre as quais se irão recolher, registar e analisar informações válidas e fiáveis" (Sarmento, 2008, p. 3). E, de acordo com o autor, o processo de investigação científica divide-se em três fases distintas: exploratória, analítica e conclusiva. A fase exploratória termina no final deste capítulo.

A fim de alcançar os objectivos definidos para a investigação, principiou-se por efectuar uma Revisão da Literatura, recorrendo, para o efeito, à pesquisa e à análise documental em obras ligadas à temática.

Simultaneamente, procedeu-se a entrevistas, aplicando o método inquisitivo, por intermédio de entrevistas semi-diretivas, das principais entidades que detêm o

conhecimento crítico nesta área de estudo e também os responsáveis pelas diversas estruturas alvo de estudo e análise, correspondendo estes capítulos à fase analítica.

Este trabalho de campo permitiu sustentar a componente teórica e responder às questões formuladas anteriormente.

1.5. Estrutura do Trabalho

Uma breve introdução, na qual é feita uma apresentação do tema, da sua pertinência, definido o objecto de estudo e os objectivos a alcançar, começa por dar forma a este trabalho.

Seguidamente, em função da metodologia adoptada, desenvolvem-se vários capítulos.

O primeiro capítulo proporciona-nos uma visão do ambiente de criação deste trabalho, no segundo capítulo, fazemos uma revisão da literatura, a definição de vários conceitos importantes e por fim analisamos quais os intervenientes da Cibersegurança em Portugal. No terceiro, expomos o método de abordagem ao problema, bem como as técnicas que nos permitiram a recolha de dados. No quarto capítulo de índole mais prática expomos os resultados obtidos no trabalho de campo, nomeadamente as entrevistas e seguidamente o levantamento das Leis relacionadas com a Cibersegurança.

De seguida, no capítulo 5 fazemos a apresentação, a análise e a discussão desses mesmos dados, procurando com isto responder às perguntas inicialmente formuladas, expor as nossas reflexões finais e recomendações.

Capítulo 2
Revisão de Literatura

2.1. Introdução

Durante a última década, o ciberespaço e os seus componentes tornaram-se numa infra-estrutura essencial de suporte à comunicação, à realização de transacções financeiras e comerciais e até à prestação de serviços públicos ao cidadão (Freire, F. e Nunes, P. 2009). Neste contexto, que vulgarmente designamos por sociedade da informação, as interacções entre indivíduos, empresas e Estado são, cada vez mais, realizadas com recurso às TIC designadamente o computador, o telemóvel e a Internet (Johnson, 2010) .

Os ataques informáticos de que a Estónia e a Geórgia foram alvo em 2007 e 2008, respectivamente, vieram alertar as autoridades nacionais e internacionais para uma nova realidade. Veio demonstrar uma nova visão, quer sobre a utilização das tecnologias no contexto de ciberconflitos de cariz assimétrico, tais como o cibercrime organizado, o hactivismo ou a ciberguerra, quer sobre os possíveis efeitos destes nas sociedades mais dependentes das TIC. Estes dois eventos mostraram ser urgente a definição de uma nova agenda global nesta área. De facto, o desenvolvimento acelerado baseado na pesquisa científica e na inovação tecnológica, que se combinam no que pode apelidar-se de tecnociência, se por um lado promete crescimento económico e prosperidade sem limites, por outro sujeita as sociedades a vulnerabilidades que, uma vez exploradas, podem ter consequências nefastas e imprevisíveis. Neste âmbito, também a dependência das TIC, a que importantes sectores de actividade estão, hoje em dia, subordinados, constitui-se como factor de preocupação. Aliás, a atentar nas situações descritas, pode estar mesmo a tomar forma uma nova linha da frente para a segurança dos Estados e dos cidadãos (Santos, 2011).

Garantir a segurança da informação no ambiente digital constitui então, cada vez mais, uma preocupação à escala mundial, seja por parte de organismos públicos, privados, universidades, empresas e até pelos cidadãos, de forma individual ou colectiva.

Na realidade, os riscos e ameaças não conhecem fronteiras de natureza geográfica, linguística, política ou qualquer outro tipo de barreiras. O que verificamos é que da mesma forma que aumenta a quantidade de informação em formato digital disponível,

nomeadamente na Internet, também se verifica um aumento contínuo das ameaças e dos ataques à segurança da informação digital, levando também a um crescimento das estratégias de promoção da segurança e redução do risco. (Campos, 2002)

Promover a segurança da informação digital é uma tarefa verdadeiramente multidisciplinar envolvendo, para além da Informática, outras áreas do conhecimento como o Direito, o Marketing, a Matemática, a Sociologia ou o comércio electrónico, só para dar alguns exemplos. Além disso, a variedade e diversidade de informação que se pretende proteger é muito vasta, podendo ser, por exemplo, bases de dados, fundos arquivísticos, dados pessoais altamente sigilosos, entre muitos outros (Silva, 2003).

Reforça-se, pois, a necessidade de definir, perante cada situação concreta ou até numa perspectiva mais abrangente, qual o tipo de protecção a aplicar, a respectiva arquitectura, os objectivos e a equação do trinómio custo, benefício e risco.

Fundamental é também conhecer as vulnerabilidades e fraquezas que possam existir, se são interna ou externas, quais as possíveis consequências e as melhores ferramentas e práticas a adoptar para as reduzir ou pelo menos prevenir e, caso se concretizem, ter um plano de contingência que permita uma rápida actuação e minimize as suas consequências (Valente, 2001).

Seguindo a sistematização relativamente ao ciberataques de Pedahzur (2009) existem três domínios de actuação face a estes últimos, designadamente o domínio da protecção simples, o domínio da prossecução criminal e o domínio da defesa do Estado. A cada um destes domínios corresponde uma perspectiva relativamente aos ciberataques, a qual determina diferenças relevantes no que respeita aos objectivos a atingir, aos principais actores envolvidos, aos meios técnicos disponíveis e ao enquadramento jurídico aplicável. Vistos a partir da perspectiva da defesa do Estado os ciberataques são entendidos como actos de guerra, pelo que a resposta se centra na acção militar, com todos os recursos disponíveis, apenas sujeita na acção, no plano nacional, à Constituição da República, à Lei do estado de Sítio e do estado de Emergência e, no plano internacional, ao Direito Internacional dos Conflitos Armados e ao Direito Internacional dos Direitos Humanos. No domínio da prossecução criminal, os ciberataques são vistos e definidos como actos criminalmente relevantes, passíveis de sancionamento dentro do edifício jurídico do respectivo país. Já para a protecção simples contribui um vasto espectro de actores com o objectivo último de proteger os activos das organizações e dos indivíduos. Esta protecção compreende todos os meios tecnológicos permitidos na lei, bem como as normas técnicas e

os instrumentos legais, e é realizada, em primeira instância, pelos donos desses activos, bem como por empresas privadas em regime de *outsourcing* e fabricantes de *hardware* e de *software* especializados, mas também pelo Estado, através das suas Forças e Serviços de Segurança (FSS) e autoridades reguladoras. Na definição de uma política de protecção do Ciberespaço, o seu centro de gravidade depende de vários factores, nomeadamente "*threat politics*", ou seja, "o processo pelo qual uma nova ameaça é introduzida na agenda política". De facto, percebe-se que os Estados com programas de contra-terrorismo, entre os quais se destacam os Estados Unidos, incluam a cibersegurança num contexto de segurança e defesa nacional, focando as atenções no desenvolvimento de meios técnicos para a monitorização do uso da internet e para a construção de capacidades militares destinadas a fazer face a ataques de larga escala (Dunn, 2005).

Por sua vez, os Estados preocupados com a importância da Internet para a economia e com o facto de esta ser gerida e operada maioritariamente por entidades privadas, colocaram o enfoque da cibersegurança no plano do combate à cibercriminalidade e da regulação e do robustecimento da resiliência das Infra-Estruturas de comunicação, independentemente do tipo de ameaça. Neste ponto de vista, a cibersegurança é vista como factor de geração de confiança no comércio electrónico e como parte integrante das políticas de desenvolvimento da designada sociedade da informação ou, mais recentemente, sociedade do conhecimento. Neste contexto, a cibersegurança é igualmente vista como um instrumento necessário à garantia da protecção da privacidade dos cidadãos. Esta perspectiva torna-se particularmente relevante quando muitos governos encaram como prioritária a desmaterialização da informação e a mediação informática entre o Estado e o cidadão, tudo factores potenciadores de um acesso desmaterializado e situado em patamares de controlo distintos da tradicional posse material de documentos em suporte de papel (Lewis. 2002).

Por outro lado, nos países com tradição no desenvolvimento de planos de protecção de Infra-Estruturas Críticas, a interdependência da Internet e das TIC, em geral com outros sectores particularmente críticos como a energia ou os transportes, elevou a cibersegurança para um patamar de relevo na estratégia de protecção dessas Infra-Estruturas face ao poder disruptivo dos ciberataques. Por este mesmo motivo o próprio Ciberespaço passou a ser classificado como infra-estrutura crítica, designando-se, normalmente, como infra-estrutura de informação críticas.

Para compreender a relativa fragilidade dos Estados face a ciberataques, bem como a vulnerabilidade das TIC em geral, há que lembrar o modo como a informática foi introduzida no contexto da gestão e operação de grandes Infra-Estruturas. Os elevados ganhos em produtividade e o baixo custo da tecnologia levaram a que, nas últimas décadas, tivéssemos assistido à informatização de grande parte das operações e processos que compõem as actividades empresariais e do Estado. As pessoas foram substituídas por computadores e programas informáticos e os arquivos de papel foram substituídos por arquivos digitais (Martins, 2003).

A especialização do pessoal informático e a necessidade de condições de funcionamento particulares levaram à criação de *datacenters* - "centros de dados" que, como o próprio nome indica, concentram numa espécie de ponto nevrálgico de computadores e redes de comunicação, as funções de monitorização, tomada de decisão e controlo remoto de todos os sistemas vitais à actividade (Lewis, 2002).

Esta informatização, realizada num contexto de maximização da funcionalidade e num momento em que os computadores pessoais e a Internet eram ainda uma miragem, quase nunca se considerou a segurança como uma prioridade.

Na realidade, as preocupações com a segurança destes sistemas centravam-se na disponibilidade de serviço (*business continuity*), na salvaguarda da informação (*backups*), no acesso físico às instalações e na ameaça da *engenharia social*, que consistia o quadro de pessoal da empresa. O advento da Internet como infra-estrutura global de comunicações de baixo custo e a banalização do computador pessoal permitiram a criação de serviços em linha e o rápido crescimento da informação digital circulante ou armazenada, alterando, de forma substancial, o paradigma da segurança informática. Esta transformação veio criar oportunidades para actores existentes e facilitar o surgimento de novos actores do crime, alargando, assim, o espectro de ameaças e dissipando as fronteiras ou os domínios de segurança existentes. A oportunidade que o Ciberespaço proporciona aos criminosos levou a que crimes comuns praticados no mundo real fossem mimetizados no mundo virtual, tirando partido do relativo grau de anonimato e da velocidade com que as suas operações podem ser realizadas, mas também da inadequação da legislação e da incapacidade das FSS para lidar com este problema novo (Libicki, 1995).

De facto, a Internet tornou-se numa infra-estrutura crucial de suporte à comunicação, à realização de transacções financeiras e comerciais e à prestação de serviços públicos ao cidadão. Existe uma crescente dependência relativamente à Internet

por parte dos diversos agentes da sociedade (empresas, bancos, escolas ou governos), o que leva a que a protecção desta infra-estrutura se esteja a tornar premente, à semelhança de outras já consideradas críticas, nomeadamente redes de distribuição de energia eléctrica e de água ou a infra-estrutura pública telefónica. Desde a forma como interagimos com o Estado (*e-government*) ou com o sector bancário (*e-banking*), até à forma como desenvolvemos as nossas guerras (*information warfare*), o palco das actividades tem-se recentrado no plano do virtual que designamos de Ciberespaço, em detrimento do plano físico (Denning, 2000).

É a combinação entre a quantidade de informação ligada em rede e a crescente complexidade dos sistemas computacionais e aplicações de suporte para os mais variados fins, que torna estes sistemas e a informação neles contida em alvos extremamente vulneráveis a ataques. Há algum tempo que estrategas e especialistas da área da segurança das redes e da informação vêm a alertar as autoridades para possíveis vulnerabilidades resultantes do rápido crescimento da Internet e da maior dependência das sociedades nesta infra-estrutura, os exemplos atrás referidos reforçam esse alerta (Arquilla and Ronfeldt, 2001).

A protecção do Ciberespaço acarreta novos e grandes desafios e muito há por fazer, quer no plano nacional, quer internacional. Com diferentes níveis de responsabilidade, tanto a indústria, como os cidadãos, como os Estados são partes interessadas na cibersegurança como garante dos bens jurídicos fundamentais.

Muito tem vindo a ser feito a nível nacional e internacional em prol desta garantia. No caso de Portugal, no entanto, é perceptível que não existe um fio condutor ou uma estratégia nacional que dê consistência e coerência a um conjunto de iniciativas individuais e desarticuladas, potenciando ineficácia das mesmas e o desperdício de recursos (Santos, 2011).

Por tudo isto, importa estudar a segurança do Ciberespaço de uma forma holística e elevar a percepção dos vários responsáveis governativos, bem como das entidades privadas, para a necessidade de acompanhar o desenvolvimento tecnológico com as políticas e as medidas de combate às novas ameaças que o mundo virtual apresenta. Este trabalho pretende dar um contributo, ainda que modesto, para a melhoria dessa percepção e responder ao que se considera ser uma necessidade da criação de uma estrutura de governação para a cibersegurança em Portugal (Ascenção, 2000).

2.2. Definição de Conceitos

Dado o nível de especificidade do tema abordado surge então a definição de conceitos ou Taxionomia para que seja possível perceber o que é discutido e comparar com outros estudos ou documentação.

2.2.1. Informação

A informação é um conjunto organizado de dados, que constitui uma mensagem sobre um determinado fenómeno ou evento. A informação permite resolver problemas e tomar decisões, tendo em conta que o seu uso racional é a base do conhecimento.

Outra perspectiva indica-nos que a informação é um fenómeno que confere significado ou sentido às coisas, já que através de códigos e de conjuntos de dados, forma os modelos do pensamento humano (Floridi, 2013).

Existem diversas espécies que comunicam entre si através da transmissão de informação para a sua sobrevivência; a diferença para os seres humanos reside na capacidade de criar códigos e símbolos com significados complexos, que conformam a linguagem comum para o convívio em sociedade.

Os dados são percepcionados através dos sentidos e, uma vez integrados, acabam por gerar a informação necessária para produzir o conhecimento. Considera-se que a sabedoria é a capacidade para julgar correctamente quando, como, onde e com que objectivo se aplica o conhecimento adquirido.

Os especialistas afirmam que existe uma relação indissolúvel entre a informação, os dados, o conhecimento, o pensamento e a linguagem (Casagrande,1999).

2.2.2. Tecnologias de Informação e Comunicação

TIC é a aplicação de computadores e equipamentos de telecomunicações para armazenar, recuperar, transmitir e manipular dados. O termo está habitualmente associado ao uso de computadores e redes de computadores, mas abrange também outras tecnologias

de distribuição de informação, como a televisão, telefones e outros aparelhos electrónicos. Existe uma forte vertente industrial associada à tecnologia da informação, tais como *hardware*, *software*, electrónica, semicondutores, internet, equipamentos de telecomunicações, comércio electrónico e outros serviços de informática (Ralston, A.2000).

Pode também ser entendido como estudo, concepção, desenvolvimento, aplicação, implementação, suporte e manutenção de sistemas de informação baseados em computadores.

O termo "tecnologia da informação", surgiu pela primeira vez num artigo de 1958 publicado na *Harvard Business Review*, onde os seus autores explicam que "a nova tecnologia ainda não tem um único nome estabelecido. Vamos chamá-lo de tecnologia da informação (TI)" (Chandler e Munday , 2011).

Pode também ser definido como os procedimentos, métodos e equipamentos para processar informação e comunicar que surgiram no contexto da Revolução Informática. Estas tecnologias agilizaram e tornaram menos palpável o conteúdo da comunicação, por meio da digitalização e da comunicação em redes para a captação, transmissão e distribuição das informações, que podem assumir a forma de texto, imagem estática, vídeo ou som. Considera-se que o advento destas novas tecnologias e a forma como foram utilizadas por governos, empresas, indivíduos e sectores sociais possibilitaram o surgimento da Sociedade da Informação (Daintith, 2012).

2.2.3. Internet

Nos anos 60 foi desenvolvida, pelo Departamento de Defesa dos EUA, a antecessora da Internet, que na altura se designou por *Advanced Resarch Project Agency Network* envolviment (ARPANET), no entanto, esta rede só começou a ser utilizada em larga escala durante os anos 70 quando os computadores militares e outros pertencentes aos meios universitários foram interligados através da rede telefónica. No início dos anos 90 a internet constituía já como uma plataforma internacional e registava mais de sete milhões de utilizadores em todo o mundo, no entanto, foi nesta década que se assistiu ao crescimento desenfreado, não só do número de utilizadores, como dos conteúdos disponíveis e das tecnologias utilizadas para acesso a esta rede de comunicação global.

No início dos anos 90, este sistema tornou-se tão complexo que é impossível actualmente determinar a sua total dimensão ou proprietários (Bell, 2001).

A Internet revolucionou o mundo das comunicações e das relações pessoais de uma maneira sem precedentes. A Internet é simultaneamente uma ferramenta mundial de radiodifusão, de disseminação de informação, um meio para colaboração e interacção entre indivíduos e seus computadores, independentemente de sua localização geográfica. (Webster, 2002).

2.2.4. Ciberespaço

O termo Ciberespaço é usado para referir o conjunto dos sistemas informáticos como *Hardware*, *Software*, redes de comunicação, equipamentos e meios de comunicação e informação neles processados e armazenada. Sinónimos comummente usados para Ciberespaço são expressões tais como: espaço virtual, mundo virtual, reino electrónico, esfera da informação, etc. O termo Ciberespaço (na sua versão anglo-saxónica cyberspace) foi cunhado em 1984, pelo escritor de ficção científica William Gibson, no seu romance, como "a consensual hallucination experienced daily by billions of legitimate operators, in everynation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data" (Gibson,1984).

Diferentemente da maioria dos termos informáticos, "Ciberespaço" não tem uma definição padrão, objectiva. Em vez disso, é usado para descrever o mundo virtual de computadores. Por exemplo, um objecto no Ciberespaço refere-se a um bloco de dados que flutuam em torno de um sistema de computadores ou rede. Com o advento da Internet, Ciberespaço estende-se agora como a rede global de computadores.

2.2.5. Cibersegurança

A cibersegurança refere-se à segurança da informação digital armazenada nas redes electrónicas, assim como a segurança das redes que armazenam e transmitem a informação.

Por vezes pode ser usada como sinónimo de segurança da informação "a protecção da informação e dos sistemas de informação de acessos não autorizados, uso, divulgação, interrupção, modificação ou destruição, confidencialidade, integridade e disponibilidade. "[1] A cibersegurança e a segurança da informação referem-se geralmente ao mesmo fim. No entanto, a segurança da informação é usado por organizações e profissionais das Tecnologias da Informação, enquanto que a cibersegurança é geralmente usada em ambientes políticos e quando as questões de segurança da informação são enquadradas como as questões de segurança nacional (Comninos, 2013).

Pode também ser definida cibersegurança como o conjunto de ferramentas, as políticas, os conceitos de segurança, salvaguardas de segurança, directrizes de gestão de risco, acções, formação, boas práticas, segurança e tecnologias que possam ser utilizadas para proteger a organização, o ciberespaço e os bens do utilizador. Ela esforça-se para garantir a estabilidade e manutenção da segurança da propriedade da organização e dos activos do utilizador contra riscos de segurança relevantes no ambiente cibernético. Primando pela disponibilidade; integridade, autenticidade e Confidencialidade (ITU, 2008).

2.2.6. Cibercrime

O Cibercrime pode ser definido de várias formas consoante os diversos autores e níveis de especificidade e amplitude. Podem ser cibercrimes "qualquer crime que é

"Integridade significa protecção contra modificação indevida ou destruição, e inclui a garantia da autenticidade da informação, confidencialidade significa preservar restrições acesso e divulgação, incluindo os meios para proteger a privacidade pessoal e propriedade da informação e disponibilidade significa garantir o acesso e uso da informação de forma oportuna e fiável" (Kissel, 2011).

cometido através de um computador ou rede, ou dispositivo de hardware. O computador ou dispositivo de hardware pode ser o agente do crime, facilitador ou alvo do crime" (Symantec Corporation, 2013).

> Independentemente da definição, a conceptualização do cibercrime envolve uma série de elementos-chave e perguntas, incluindo onde são materializados os actos de execução criminais, no mundo real ou digital (e quais tecnologias que estão envolvidas), a motivação do crime e quem está envolvido na realização dos actos. O cibercrime resulta, em grande medida, da aplicação da capacidade técnica destes criminosos na prática quer de crimes clássicos, quer de novos crimes proporcionados pelas novas tecnologias (Martins, 2003).

Estes crimes podem ser divididos em três grupos: crimes convencionais realizados com recurso a computador; crimes convencionais em que o computador não é o instrumento principal da actividade mas onde o meio de realização de prova assume a forma digital; e crimes em que o alvo são os sistemas informáticos (Grabosky, 2004). Como exemplo de cibercrimes, temos o furto de telecomunicações, a intercepção ilegal de comunicações, o furto de propriedade intelectual, o *cyber-stalking*, o branqueamento de capitais e evasão fiscal electrónicos, o vandalismo electrónico que inclui o ciberterrorismo, a extorsão e a sabotagem, a fraude informática, a contrafacção de cartões, o furto de identidade, os crimes de conteúdo ofensivo, a espionagem electrónica e a utilização não autorizada de recurso informático (Broadhurst and Chantler, 2006).

2.2.7. Infra-Estruturas Críticas Nacionais

Uma Infra-estrutura crítica Nacional pode ser definida como uma componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem -estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções.

Em termos gerais, estas estruturas críticas materializam-se no sector da energia, designadamente as Infra-Estruturas e instalações de produção e de transporte de electricidade, Infra-Estruturas de produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos e Infra-Estruturas de produção, refinação, tratamento,

armazenagem e transporte de gás por gasodutos e terminais para gás natural em estado líquido. No sector dos transportes, designadamente: rodoviários; ferroviários; aéreos; transportes por vias navegáveis interiores; marítimos, incluindo de curta distância, e portos.[2]

Para serem consideradas Infra-Estruturas Críticas Nacionais tem de ser verificados diversos critérios como a possibilidade de ocorrência de acidentes, avaliada em termos de número potencial de feridos ou vítimas mortais, o impacto económico estimado, avaliado em termos de importância dos prejuízos económicos e da degradação de produtos ou serviços, incluindo também os potenciais efeitos ambientais. Os efeitos previsíveis no domínio público, avaliados em termos de impacto na confiança das populações, sofrimento físico e perturbação da vida quotidiana, incluindo a perda de serviços essenciais. (Mendes, 2012)

2.2.8. Caracterização da ameaça

A ameaça é segundo o General Cabral Couto "qualquer acontecimento ou acção (em curso ou previsível) que contraria a consecução de um objectivo e que, normalmente, é causador de danos, materiais ou morais. As ameaças podem ser de variada natureza". A ameaça é causada por uma vontade consciente, com vista à prossecução de objectivos próprios, e traduzem-se numa situação de coação. A coação, por sua vez, pode ser psicológica, diplomática, de política interna, económica e militar (Couto, 1988).

A ameaça pode ser ainda entendida como " qualquer acontecimento ou processo que leva à perda de vida ou à redução de expectativas de vidas humanas em larga escala e que ponha em causa a unidade do sistema internacional, ameaçando a segurança internacional" (Loureiro, 2000).

O conjunto das actividades que podem tirar proveito, de uma ou outra forma, da forte dependência dos Estados e das empresas relativamente ao uso das TIC, afectando negativamente o seu funcionamento. Pode ser dividido em várias categorias de acordo com a motivação e o perfil dos seus autores, a saber: cibercrime, desobediência civil electrónica e hacktivismo, ciberterrorismo e ciberguerra. O espectro de motivações observadas

[2] Cf. Decreto-Lei n.º 62/2011de 9 de Maio

estende-se desde o gozo pessoal e o estatuto dentro de um grupo decorrentes da experimentação de técnicas de *Hacking*, numa das extremidades, até à obtenção de uma vantagem competitiva de um Estado relativamente a outro, na outra (Lewis, 2002).

O perfil dos autores pode ser caracterizado através do binómio compostos pelo grau de conhecimentos técnicos e pelo nível de profissionalismo ou associação criminosa.

Também de registar a multiplicidade de factores de risco e de ameaças relacionadas com o ciberespaço, designadamente no âmbito do hactivismo, da espionagem e do terrorismo. Sobressai, a este propósito, as actividades de agentes e organizações que, usando as plataformas cibernéticas, têm a motivação e as capacidades para desencadear operações que visam corromper ou desvirtuar o arquétipo securitário do nosso país e das organizações internacionais de que Portugal é membro.

Devem referir-se as acções dos grupos extremistas violentos, cabendo notar, também neste espectro, a importância dos fenómenos de radicalização através da Internet. (RASI, 2012)

2.3. Responsabilidade da Cibersegurança em Portugal

Nesta secção pretendemos elencar as entidades relevantes para a cibersegurança em Portugal e descrever o seu papel neste contexto. Para o efeito foi desenhada uma matriz que visa representar o papel e o contributo de cada uma dessas entidades para o esforço de cibersegurança nacional. Foram considerados como eixos para a matriz, por um lado o plano de responsabilidade, seja ele o plano político, o plano estratégico ou o plano operacional. Por outro, consideramos os seis eixos de intervenção explanados no capítulo anterior, nomeadamente a normalização e certificação, a formação e consciencialização, o alerta e resposta à emergência, a protecção de Infra-Estruturas Críticas, o combate ao cibercrime e a investigação e desenvolvimento.

A informação apresentada foi recolhida a partir de *web sites* institucionais, leis orgânicas, bem como do relatório da ENISA sobre a Cibersegurança em Portugal de 2011. Com esta metodologia pretendeu criar-se um quadro que ilustra as responsabilidades e actividades das entidades públicas e privadas que contribuem para a cibersegurança nacional. Da análise da Figura nº1 podem identificar-se sobreposições e lacunas que sustentam as propostas de articulação e de cooperação à frente apresentada.

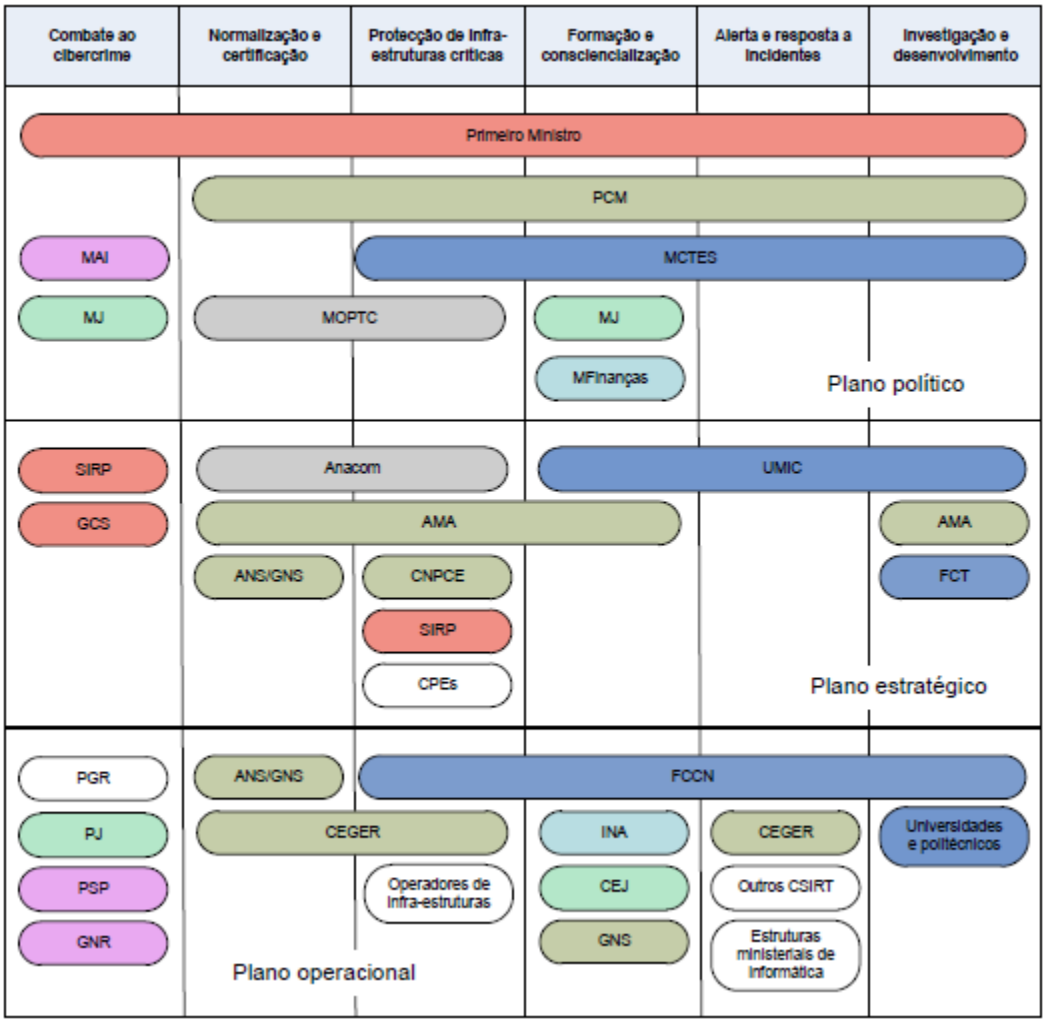


Figura nº 1 - Entidades responsáveis pela cibersegurança em Portugal (Santos, 2011)

2.3.1. Agência para a Sociedade do Conhecimento

A UMIC – Agência para a Sociedade do Conhecimento, IP é o organismo público português com a missão de coordenar as políticas para a sociedade da informação e mobilizá-la através da promoção de actividades de divulgação, qualificação e investigação. Promover o desenvolvimento tecnológico e a criação e divulgação de boas práticas. Estimula o desenvolvimento da E-Ciência, exercendo a sua actividade sob a tutela e superintendência do Ministro da Educação e Ciência. Das suas atribuições destacam-se a promoção da cibersegurança e da privacidade no uso da Internet e das TIC; a promoção de

projectos que contribuam para a massificação do acesso à Internet de banda larga em Portugal e à sua utilização efectiva por todos os cidadãos. [3]

2.3.2. Agência para a Modernização Administrativa

A Agência para a Modernização Administrativa (AMA)- foi criada no âmbito do Programa para a Reestruturação da administração central do Estado em através da lei orgânica da Presidência do Conselho de Ministros, aprovada pelo Decreto-Lei n.º 202/2006, de 27 de Outubro.

De entre as atribuições da AMA destacam-se, no contexto deste trabalho, a responsabilidade desta no contexto do E-Government, nomeadamente o apoio ao governo na definição das linhas estratégicas e das políticas gerais relacionadas com a administração electrónica e distribuição de serviços públicos; a coordenação do processo de decisão de projectos em matéria de investimento público; a promoção e realização de estudos, análises estatísticas e prospectivas e estimular actividades de investigação, de desenvolvimento tecnológico e de divulgação de boas práticas, na área da administração electrónica; a definição de políticas transversais e regras, com carácter vinculativo, em matéria de TIC na administração pública e coordenar a sua execução através da dinamização de uma rede interministerial de agentes das tecnologias de informação e comunicação; e, de uma forma geral, promover a evolução da actual infra-estrutura tecnológica bem como a racionalização de custos de comunicação.

Das múltiplas iniciativas e projectos salienta-se a rede interministerial para as TIC, que inclui o tema da segurança nos seus objectivos de partilha de boas práticas ou o cartão de cidadão e a plataforma de interoperabilidade como instrumentos de iteração em segurança entre o cidadão e a administração pública.

A AMA depende da Presidência do Conselho de Ministros através da Secretária de Estado da Modernização Administrativa.

[3] Informação disponível em http://www.umic.pt/ e Decreto-Lei n.º 153/2007, de 27 de Abril

2.3.3. Centro de Gestão da Rede Informática do Governo

O Centro de Gestão da Rede Informática do Governo - CEGER – desempenha um papel de extrema importância no contexto da segurança das comunicações e da informação do governo e assegura algumas funções de segurança informática transversais ao Estado, nomeadamente: presta apoio de consultoria aos membros do governo e seus gabinetes em matérias de tecnologias de informação, de comunicações e de sistemas de informação; promove, acompanha e coordena a utilização de informação e de comunicações pelos gabinetes governamentais; garante a gestão da rede do governo e vela pela sua segurança e pela segurança da informação e das bases de dados. Colabora ainda em estudos e na implementação de processos e procedimentos organizativos e funcionais nos gabinetes dos membros do governo.

Adicionalmente foi-lhe conferida a gestão operacional do Sistema de Certificação Electrónica do Estado (SCEE) e o papel de entidade certificadora de plataformas electrónicas no âmbito do código dos contratos públicos.

Igualmente importante nas atribuições do CEGER é a sua responsabilidade técnica pela operação do registo de nomes DNS para -gov.pt- do qual depende o funcionamento de boa parte das comunicações electrónicas do Estado

.

2.3.4. Órgãos Ministeriais de TIC

O Estado português possui uma miríade de centros de informática. Quase todos os ministérios têm na sua estrutura orgânica uma entidade com a responsabilidade pelas comunicações e sistemas de informação dos restantes organismos por eles tutelados. São exemplos deste tipo de estruturas o Instituto das Tecnologias de Informação na Justiça do Ministério da Justiça, o Instituto de Informática do Ministério do Trabalho e da Segurança Social, a Direcção- Geral de Informática e Apoio aos Serviços Tributários e Aduaneiros e o Instituto de Informática do Ministério das Finanças, o Instituto de Gestão Informática e Financeira do Ministério da Saúde ou a Unidade de Tecnologias de Informação de Segurança do Ministério da Administração Interna.

Cada um destes organismos realiza a gestão e a operação das redes, dos sistemas e da informação dos serviços sob a responsabilidade do respectivo órgão tutelar. A segurança destas redes e sistemas é feita directamente ou subcontratada no mercado.

2.3.5. Conselho Nacional de Planeamento Civil de Emergência

O Conselho Nacional de Planeamento Civil de Emergência - CNPCE - tem como missão preparar os sectores estratégicos do País e o apoio às Forças Armadas para fazer face a situações de crise e de guerra. Para tal, o CNPCE propõe e coordena as políticas de planeamento civil de emergência; estabelece planos e normas com vista a potenciar a resposta nacional a situações de crise e de guerra; coordena as componentes e as capacidades não militares da defesa e o apoio civil às Forças Armadas; e promove a cooperação internacional na área do planeamento civil de emergência e da gestão de crises.

O CNPCE coordena o Sistema Nacional de Planeamento Civil de Emergência, foi criado pelo Decreto-Lei n.º 153/91 de 23 de Abril e alterado pelo Decreto-Lei n.º 128/2002, de 11 de Maio. Nele insere-se a Comissão de Planeamento de Emergência do Ciberespaço, cujo presidente se encontra por nomear pelo Ministro da Ciência e da Tecnologia e de cujas atribuições se destacam a elaboração e a submissão à aprovação da tutela de diplomas, planos, procedimentos e outras disposições que minimizem as vulnerabilidades detectadas do sector; a elaboração de estudos e informações; o apoio à representação nacional e à participação nos trabalhos e outras actividades sectoriais nos órgãos pertencentes à OTAN, UE, ONU e em outros organismos internacionais congéneres; a proposta de legislação interna adequada às necessidades nacionais decorrentes de compromissos assumidos em instâncias internacionais e a realização e participação em exercícios e treinos visando a melhoria da preparação do sector em situações de anormalidade.

A actividade de Planeamento Civil de Emergência tem como um dos principais pilares a organização e a preparação dos diferentes sectores estratégicos para fazer face a quaisquer situações de anormalidade, acção que implica necessariamente o aumento da resiliência das Infra-Estruturas Críticas e da garantia do fornecimento dos bens e serviços de que necessitam para funcionar.

Neste campo, o CNPCE desenvolve um Programa Nacional para a Protecção de Infra-Estruturas Críticas, assegurando a representação internacional nesta área. Este rograma tem como objectivos a identificação e classificação das Infra-Estruturas fundamentais para o normal funcionamento do país e o bem-estar da sua população, ou ainda para o manter em níveis de funcionamento aceitáveis, em situação de crise; assim como a identificação e a avaliação das vulnerabilidades das Infra-Estruturas identificadas, face às principais ameaças passíveis de as atingir; estudo e apoio à implementação de medidas de prevenção e de reforço da resiliência com vista a conter os riscos em níveis considerados aceitáveis.

2.3.6. Autoridade Nacional de Comunicações

A Autoridade Nacional de Comunicações (ICP-ANACOM) é a entidade reguladora do sector das comunicações em Portugal. Para o contexto da cibersegurança são importantes as suas atribuições nas áreas da regulamentação e supervisão do sector das telecomunicações e do comércio electrónico nomeadamente: coadjuvar o governo, a pedido deste ou por iniciativa própria, na definição das linhas estratégicas e das políticas gerais das comunicações e da actividade dos operadores de comunicações, incluindo a emissão de pareceres e elaboração de projectos de legislação no domínio das comunicações; promover a normalização técnica, em colaboração com outras organizações, no sector das comunicações e áreas relacionadas, promover processos de consulta pública e de manifestação de interesse, nomeadamente no âmbito da introdução de novos serviços ou tecnologias; participar na definição estratégica global de desenvolvimento das comunicações, nomeadamente no contexto da convergência das telecomunicações, dos meios de comunicação social e das tecnologias da informação, realizando os estudos adequados para o efeito; colaborar na definição das políticas de planeamento civil de emergência do sector das comunicações; e assegurar a representação técnica do Estado Português nos organismos internacionais congéneres, quando de outro modo não for determinado.

O ICP-ANACOM assegura a representação portuguesa em vários fora que tocam aspectos relativos à cibersegurança. De entre estes destacam-se o *Working Party for Information Security Privacy* do Comité das Políticas de Informação, Informática e

Telecomunicações instância, da Organização para a Cooperação e Desenvolvimento Económico (OCDE) que analisa os aspectos políticos resultantes do desenvolvimento e aplicação de tecnologias e serviços na área da informação, informática e comunicações; o *Informal IRG Working Group on Information Security*, onde são trocadas experiências entre as várias autoridades reguladoras das comunicações europeias; a Agenda Global para a Cibersegurança do ITU, o órgão das Nações Unidas dedicado aos assuntos das tecnologias da informação e da comunicação; e o *European Forum of Member States* para matérias relacionadas com o programa europeu para a protecção de Infra-Estruturas Críticas da informação. O ICP- ANACOM é igualmente membro do *European Telecommunications Standards Institute*, entidade europeia responsável pela produção de normas para o sector das telecomunicações, com particular relevo na área das comunicações móveis.

O Ministro das Obras Públicas, Transportes e Comunicações tem a tutela funcional e patrimonial da ANACOM, sendo a definição das linhas de orientação e dos domínios prioritários da sua acção exercida em articulação com o Ministro de Estado e da Presidência.

2.3.7. Autoridade Nacional de Segurança / Gabinete Nacional de Segurança

O Gabinete Nacional de Segurança (GNS) é dirigido pela Autoridade Nacional de Segurança (ANS) a quem compete superintender tecnicamente os procedimentos da administração pública e garantir o cumprimento das medidas para garantia da segurança das matérias classificadas nacionais ou da responsabilidade nacional, designadamente as das organizações internacionais de que Portugal é parte, bem como exercer a autoridade de credenciação de pessoas e empresas para acesso e manuseamento dessas mesmas matérias. A ANS é igualmente a entidade credenciadora competente para a credenciação e a fiscalização das entidades certificadoras compreendidas no SCEE. No quadro das competências do GNS, destacam-se a acreditação e a certificação de segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de matérias classificadas; a promoção do estudo, investigação e difusão das normas e procedimentos de segurança aplicáveis à

protecção e salvaguarda das matérias classificadas, propondo a doutrina a adoptar por Portugal na matéria e a formação de pessoal especializado nesta área da segurança.

O GNS funciona no âmbito da Presidência do Conselho de Ministros, junto doGabinete Coordenador de Segurança. A ANS funciona na dependência directado Primeiro-Ministro.

2.3.8. Centro Nacional de Cibersegurança

A Resolução do Conselho de Ministros nº 12/2012 atribui ao GNS no âmbito da medida 4 do plano global estratégico de racionalização e redução de custos com as Tecnologias de Informação e Comunicação a missão de coordenação com todas as entidades relevantes da definição de implementação de uma estratégia nacional de segurança da informação (ENSI), que compreende a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (CNC).

A Comissão Instaladora do CNC no cumprimento do mandato que lhe foi atribuído pela Resolução do Conselho de Ministros nº 42/2012 aprovou no mês de julho de 2012 um relatório com uma proposta para a criação de um CNC, que terá como missão contribuir para que Portugal use o Ciberespaço de uma forma mais livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional.

2.3.9. Sistema de Segurança Interna

O Sistema de Segurança Interna (SSI), foi criado pela revisão de 2008 da Lei de Segurança Interna. São órgãos do SSI o Conselho Superior de Segurança Interna, o Gabinete Coordenador de Segurança e o Secretário-Geral do SSI.

Cabe ao Gabinete Coordenador de Segurança estudar e propor ao Secretário- Geral políticas públicas de segurança interna e estratégias e planos de acção nacionais na área da prevenção da criminalidade. Este Gabinete é ainda responsável pela elaboração do Relatório Anual de Segurança Interna.

Ao Secretário-Geral cabe, de particular importância para a cibersegurança, a responsabilidade da articulação das FSS e pela gestão de incidentes táctico-policiais graves, onde se incluem os ataques contra IC ou destinadas ao abastecimento e satisfação de necessidades vitais da população.

Refira-se ainda que no âmbito das suas competências de coordenação, cabe ao Secretário-Geral estabelecer os mecanismos de articulação entre as várias FSS, com os organismos congéneres e com outras entidades, públicas e privadas, relevantes na área da segurança.

O Secretário-Geral do SSI funciona na directa dependência do Primeiro-Ministro ou, por sua delegação, do Ministro da Administração Interna.

2.3.10. Sistema de Informações da República Portuguesa

O Sistema de Informações da República Portuguesa (SIRP) e os seus serviços de informações - o Serviço de informações e Segurança (SIS) e o Serviço de Informações Estratégicas de Defesa -, desempenham um papel fundamental na prevenção da criminalidade grave e das ameaças susceptíveis de fazer perigar a segurança nacional, nas suas vertentes de segurança interna e defesa nacional.

O Secretário-Geral do SIRP funciona na directa dependência do Primeiro-Ministro ou, por delegação, num membro do governo da Presidência do Conselho de Ministros.

2.3.11. Policia Judiciária

A Polícia Judiciária (PJ) é o principal órgão de polícia criminal em matéria de cibercrime. A PJ tem por missão coadjuvar as autoridades judiciárias na investigação, desenvolver e promover as acções de prevenção, detecção e investigação da sua competência ou que lhe sejam cometidas pelas autoridades judiciárias competentes.

De entre as suas atribuições destacam-se a realização das acções, que antecedem o julgamento e que requerem conhecimentos ou meios técnicos especiais, a promoção e a realização de acções - destinadas a fomentar a prevenção geral e a reduzir o número de vítimas da prática de crimes.

A PJ, nomeadamente a sua Secção de Investigação da Criminalidade Informática e Tecnológica da Directoria de Lisboa e Vale do Tejo, é ainda o órgão competente para efeitos de cooperação internacional e o ponto de contacto permanente previstos na Lei do Cibercrime (LC) e assegurar o funcionamento dos gabinetes da Interpol e Europol para os efeitos da sua própria missão e para partilha de informação.
A PJ depende hierarquicamente do Ministério da Justiça.

2.3.12. Fundação para a Computação Científica Nacional

Operado pela FCCN, o serviço de resposta a incidentes de segurança *Computer Emergency Response Team* de Portugal (CERT.PT) foi criado em 1993 e acreditado pelo órgão *Trusted Introducer* da rede de *Computer Security Incident Response Team* (CSIRT) europeia em maio de 2004 e pelo *Forum of Incident and Security Teams* em abril de 2011. O CERT.PT tem como missão a minimização de danos resultantes de incidentes de segurança das redes e da informação, assentando num conjunto de serviços pró-activos e reactivos, nomeadamente o apoio a utilizadores de sistemas informáticos na resolução de incidentes de segurança, aconselhando procedimentos, analisando artefactos e coordenando acções com as entidades envolvidas, a reunião e disseminação de um conjunto de informação relevante sobre vulnerabilidades e recomendações referentes a potenciais riscos de segurança e actividades maliciosas em curso, e a promoção da criação de novas equipas CSIRT e da coordenação nacional entre estas, assim como da articulação com outras entidades relevantes no contexto da segurança no Ciberespaço. O CERT.PT tem vindo a promover a criação de uma rede nacional de CSIRT e de pontos de contacto de segurança, celebrando acordos com entidades relevantes nesta área, nomeadamente prestadores de serviços Internet, entidades bancárias

2.3.13. CERT.PT

O CERT.PT tem como missão contribuir para o esforço de cibersegurança nacional nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de

alertas e recomendações de segurança e na promoção de uma cultura de segurança em Portugal.

A nível nacional o CERT.PT tem vindo a promover a criação de novas CSIRT (serviços de resposta a incidentes de segurança informática) através de protocolos de cooperação com os principais operadores de telecomunicações e outras entidades relevantes com vista à criação de uma rede nacional e cooperação efectiva nas áreas da segurança informática.

Capítulo 3
Metodologia

3.1. Introdução

Concluída a revisão de literatura, e com vista a alcançar os objectivos de investigação propostos, foi adoptado o método científico que se define como "o processo racional que se emprega na investigação" (Carvalho, 2009, p. 84) sendo necessário segundo Sarmento (2008, p. 3), "(…) recolher, registar e analisar informações válidas e fiáveis", que nos permitam dar resposta às questões inicialmente formuladas para a presente investigação

Face ao grau de complexidade do tema abordado e a abordagem holística feita, foi necessário recorrer dois métodos de investigação. Inicialmente, a utilização de um método quantitativo, que se materializou na recolha de documentação, maioritariamente no âmbito legal mas também, e, em complemento com o anterior, um método qualitativo ou inquisitivo, que se traduziu na realização de entrevistas realizadas aos especialistas na área a exercer funções nos cargos chave para a resposta aos objectivos de investigação permitindo ao investigador compreender melhor o fenómeno a estudar. Uma das formas de se realizar essa investigação consiste na recolha de dados, consubstanciada numa pesquisa de campo (Hill e Hill, 2002).

3.2. Procedimentos e técnicas

Este trabalho centra-se numa investigação qualitativa, e como tal recorremos a duas técnicas de recolha de informação: a análise documental e a entrevista.

Para dar sustentabilidade à investigação, empreendeu-se uma pesquisa bibliográfica e documental em várias bibliotecas e de vários repositórios *on-line*. Este primeiro método resulta da obtenção de dados através da análise documental, ou seja "(…) uma operação ou um conjunto de operações visando representar o conteúdo de um documento sobre a forma diferente da original a fim de facilitar, num estado ulterior, a sua consulta e referenciação" (Bardin, 2008, p. 47).

Por outro lado, as entrevistas possibilitam uma resposta aberta, dando possibilidade ao entrevistado uma resposta livre, podendo ainda ser reorientada pelo entrevistador.

No que concerne às entrevistas foram realizadas entre os dias de 15 a 24 de Julho 2013, sendo realizadas no total quatro entrevistas semiestruturadas do tipo intensivo, ou

seja a entrevista centra-se num indivíduo. Cada entrevistado recebeu um guião[4] de entrevista com a respectiva carta de apresentação e as questões que lhe iriam ser colocadas e sem limite de tempo possibilitando maior liberdade, o que permite que o entrevistado exponha os seus pontos de vista (Sousa e Baptista, 2001).

3.3. Entrevistas

Sendo a entrevista uma abordagem qualitativa importa referir que o seu objectivo não é obter dados estatísticos (Guerra, 2006), mas os depoimentos de quem detém o conhecimento prático nesta área e ocupa cargos de responsabilidade nesta mesma área na GNR. Sendo que para cumprir com o objectivo de recolher dados recorremos à observação indirecta, onde o investigador a fim de obter informações interroga o sujeito, que produz informação (Quivy & Campenhoudt, 2008). Este método revelou-se imprescindível para a obtenção de informação capaz de satisfazer os objectivos predeterminados e conferiu ao investigador a possibilidade de aceder a dados com "(…) um grau máximo de autenticidade e profundidade" (Quivy e Campenhoudt, 2008, p. 192). Privilegiou-se este método como método de recolha de dados porque a Cibersegurança na GNR é uma área muito restrita de emprego de pessoal e não seria possível elaborar inquéritos em número suficiente para analisar os dados de forma a produzir resultados válidos do ponto de vista científico e porque a recolha de documentação não satisfez os objectivos de investigação. As entrevistas são utilizadas para analisar um problema específico, como o funcionamento de uma organização (QUIVY & CAMPENHOUDT, 2008), neste caso, a Cibersegurança e as Estruturas Críticas. As entrevistas tinham por objectivo recolher o conhecimento e a experiência dos militares da Guarda que, pelas funções que desempenham, têm um papel decisivo no que respeita à Cibersegurança e a gestão e segurança das Infra-Estruturas Críticas da Guarda. Por outro lado, constituiu-se num meio capaz de preencher os requisitos defendidos por Coutinho (2011, p. 90), segundo o qual "todo e qualquer plano de investigação, seja ela de cariz quantitativo, qualitativo ou multi-metodológico, implica uma recolha de dados originais por parte do investigador". O método, da entrevista foi semiestruturado de forma a que se baseasse em perguntas-guia (Quivy & Campenhoudt,

[4] Ver Anexo 1

2008) mas que garantisse liberdade suficiente para opinar sobre as diversas temáticas procurando que "(…) o entrevistado responde às perguntas do guião, mas também pode falar sobre outros assuntos relacionados" (Sarmento, 2008, p. 18), que estão plasmadas no guião de entrevista que é o "suporte da entrevista" (Quivy & Campenhoudt, 2008, p. 181), elaborado sempre "em função dos objectivos que decorrem da problematização" (Guerra, 2006, p. 53).

Todas as entrevistas foram realizadas presencialmente, e após o devido consentimento, foram gravadas, de forma a permitir a sua posterior transcrição e análise, mantendo a fiabilidade das respostas que, de outra forma, não se conseguiria. O meio utilizado para essa gravação foi o gravador Samsung Galaxy Ace S58530.

Finalizadas as entrevistas, foram transcritas recorrendo ao programa informático *Express Scribe Pro* e para efeitos de tratamento da informação recolhida, procedeu-se a uma análise qualitativa do seu conteúdo. A análise de conteúdo, melhor do que qualquer outro método de trabalho permite "(…) quando incide sobre um material rico e penetrante, satisfazer harmoniosamente as exigências do rigor metodológico e da profundidade inventiva, que nem sempre são facilmente conciliáveis" (Quivy e Campenhoudt, 2008, p. 227). Para o efeito, à imagem do que é defendido por Guerra (2010, p. 73), para cada questão criou-se uma "grelha vertical", na qual, de forma fidedigna, se reproduziram as respostas dos entrevistados, através de uma síntese dos seus discursos. Segundo o Autor, estes quadros são bastantes úteis, pois permitem reduzir a quantidade de informação a trabalhar e, ainda, proceder à sua comparação, no sentido de encontrar aspectos comuns ou divergentes entre as diferentes entrevistas. A análise descrita permite, deste modo, dar resposta às hipóteses da investigação.

3.4. Caracterização da amostra

A amostra é constituída por um grupo de Oficiais da GNR[5] directamente envolvidos na vertente da Cibersegurança na GNR, com vasta formação nesta área do conhecimento inclusive com bibliografia publicada e actualmente a exercer funções no Comando Geral da Guarda. De referir que utilizaremos o termo "amostra" num sentido não probabilístico para nos referirmos ao nosso universo de análise qualitativa, opção da maioria dos autores (GUERRA, 2006). Mas sim de acordo com Freixo (2011) uma amostra por selecção racional, que origina uma amostra de tipo não probabilístico em que os elementos da população são escolhidos por causa da correspondência entre as suas características e os objectivos do estudo.

Quadro nº 1

Nº da Entrevista	Nome do Entrevistado	Posto	Função
1	Ricardo Bessa	Major	Chefe da Secção de Recursos Humanos e Chefe da Secção de Justiça da Secretaria Geral da GNR
2	Rogério Raposo	Capitão	Chefe da Repartição de Aplicações e Sistemas
3	Paulo Santos	Major	Chefe da Repartição Produção e Desenvolvimento
4	Carlos Pimentel	Major	Repartição de Segurança

[5] Quadro 1

Capitulo 4
Análise e discussão dos resultados

4.1. Introdução

Neste Capítulo, que se considera um dos mais importantes deste trabalho, está prevista a apresentação, análise e discussão dos resultados do trabalho empírico, nomeadamente, os resultados obtidos através da análise de conteúdo das entrevistas e da recolha documental. As análises aqui expostas foram alvo de uma organização prévia, utilizando diferentes meios de tratamento que foram já referenciados no capítulo anterior. Para Guerra (2006, p. 53) existe "a necessidade de comparabilidade entre os sujeitos e o evitamento da descrição" e para tal, houve um esforço nesse sentido encontrando-se neste capítulo apenas um resumo dos aspectos mais importantes a fim de "facilitar a comparação longitudinal das entrevistas" (Guerra, 2006, p. 73) e permitir a construção das possíveis respostas às questões de partida. Foram também criadas sinopses[6] das entrevistas, com o objectivo de "Reduzir o montante de material a trabalhar identificando o *corpus* central da entrevista" (Guerra, 2006, p. 73).

Juntando todas as respostas dos quatro entrevistados por pergunta, ou seja, analisando cada resposta a cada pergunta, foram construídos quadros com as menções mais importantes das respostas dos entrevistados, para posterior comparação de ideias.

4.2.1. Análise à questão n.º 1

No quadro n.º 2, é apresentada a argumentação relativa à **Questão n.º 1 – " O que é o Ciberespaço e que desafios coloca às sociedades modernas e ao ambiente de Informação?"**

[6] Apêndice 2

Quadro nº 2

Entrevistado	Ideias Chave
1	- Apesar do Ciberespaço ser um conceito abstracto ele materializa-se numa componente física A informação existe fisicamente em algum lado, existem outros equipamentos que asseguram a comunicação e todos estes patamares devem ser salvaguardados. Cada um destes pontos pode constituir vulnerabilidades e quebras de segurança. - O problema da partilha, é que muitas vezes se partilha mais do que queremos, sem nos apercebermos. E tudo aquilo que nós disponibilizamos no Ciberespaço, jamais conseguimos apagar completamente se o quisermos. Independentemente do tipo de informação, pois mesmo que o apaguemos a informação já se propagou pelo Ciberespaço e é impossível garantir que ela tenha sido mesmo eliminada.
2	- O Ciberespaço é a auto-estrada da comunicação virtual, que liga as pessoas, os sistemas através de nós e redes de comunicação. É um novo espaço de interacção humana que já tem uma importância enorme sobretudo no plano económico e científico e, certamente, essa importância tem consequências a nível da segurança que a sociedade não pode ignorar.
3	O Ciberespaço é uma evolução da internet, no sentido de aliar a tecnologia à sociedade surgindo então a sociedade de informação. - "O Ciberespaço é o estado tecnológico mais aproximado da natureza humana." Está bem presente o dualismo entre o bem e o mal. - "No Ciberespaço circula informação e informação é poder. Este poder pode servir vários fins como por exemplo a ciberguerra"

4	- Rede que interliga estes meios digitais sejam eles servidores, computadores, telemóveis, tablets ou terminais de pagamento automático. Assenta numa rede que os dados digitais materializam transacções económicas ou sociais. - Não há sistemas 100% seguros, o que se pode fazer é criar barreiras de protecção para salvaguardar a integridade deste sistema. - Desafio de encontrar o compromisso entre a segurança do sistema e a sua funcionalidade e custo.

Análise da questão n.º 1

A análise das respostas à Questão n.º1 revela que o Ciberespaço é conceito dual na sua essência. Pois é algo abstracto no que diz respeito à informação que circula, os dados transmitidos não são palpáveis. No entanto existe um esqueleto que suporta toda esta nuvem de informação, constituído por servidores, bancos de dados, nós de comunicações e todos os aparelhos informáticos e electrónicos com capacidade de se ligarem a esta rede. O Ciberespaço é uma componente da nossa sociedade que teve um desenvolvimento exponencial no último século, e que está relacionado com todos os aspectos da vivência da sociedade na era da Informação. Fazendo uma análise introspectiva, neste momento, a nossa sociedade e o Ciberespaço são realidades indissociáveis.

Este facto tem repercussões ao nível da segurança pois sendo que "O Ciberespaço é o estado tecnológico mais aproximado da natureza humana." As condutas criminosas praticadas no mundo real estão a ser praticadas de forma homóloga no Ciberespaço e cada vez mais, esta tipologia de crimes torna-se mais organizada, complexa e tecnologicamente avançada.

4.2.2. Análise à questão n.º 2

No quadro n.º 3, é apresentada a argumentação relativa à **Questão n.º 2 – O que é e como é possível garantir a Cibersegurança das Infra-Estruturas Críticas Nacionais?**

Quadro nº 3

Entrevistado	Ideias Chave
1	- Um Sistema Crítico tem que garantir a continuidade do Serviço, isso pode passar pela criação de Sistemas Redundantes. - Segurança física, controlo de acessos tem de respeitar certos protocolos e aspectos de segurança. Os utilizadores são elementos do Sistema e se não fizer uma utilização instruída e consciente da sua responsabilidade para a segurança, pode ser um dos pontos mais frágeis para a segurança. - A segurança é uma responsabilidade de todos.
2	- Segurança aplicacional e Segurança de Rede através de Fire-walls de rede, sendo esta fechada e encriptada, não sendo possível aceder fora dos nossos terminais. - Nas aplicações utiliza-se com credenciação, o que permite que todos os acessos internos sejam auditáveis, ou seja, qualquer alteração feita fica associada a um Utilizador podendo este ser responsabilizado pelas suas acções no sistema.
3	- Definindo um Conceito de Estratégia de Defesa das nossas Infra-Estruturas Críticas. - Certificação e aplicação de normas internacionais para o uso das TIC - Acções de formação e consciencialização. Quer ao nível privado quer ao nível público porque a cibersegurança é uma responsabilidade partilhada. - Numa perspectiva reactiva tem de haver uma resposta a incidentes. - Com um *f*uncionamento eficaz do aparelho legislativo nomeadamente na área do Código Penal (CP) e Código do Processo Penal (CPP), não só a nível Internacional mas também a transição para o normativo nacional.

4	Falta um levantamento do conjunto das Estruturas Críticas Nacionais de Informação e das suas necessidades específicas de segurança. CERT.pt A Cibersegurança deve ser promovida em três frentes: 1. A frente repressiva, em que é necessário capacitar os Órgão de Polícia Criminal (OPC) para o travar e as autoridades judiciais para o punir. 2. Formação das pessoas que estão ligadas ao aparelho judicial e policial 3. Formação e sensibilização e consciencialização da sociedade em geral

Análise da questão n.º 2

É do entender geral dos entrevistados que a Cibersegurança é um problema multifacetado e que exige uma resposta holística e definida pelo poder político. A necessidade da adopção de medidas surge pela importância que a UE tem dado a esta temática. Em especial a Comissão Das Comunidades Europeias[7] que estabelece a estratégia de cibersegurança que se articula em cinco prioridades estratégicas, que abordam os desafios acima destacados: Garantir a resiliência do ciberespaço, reduzir drasticamente a cibercriminalidade, desenvolver a política e as capacidades no domínio da Ciberdefesa no quadro da Política Comum de Segurança e Defesa (PCSD), desenvolver os recursos industriais e tecnológicos para a cibersegurança, estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da EU.

Ao nível nacional existe uma proposta de Estratégia Nacional de Cibersegurança enquadrada no âmbito da *European Network and Information Security Agency* (ENISA)
E estabelece os três objectivos estratégicos: garantir a segurança no ciberespaço, fortalecer a cibersegurança das infra-estruturas críticas nacionais, defender os interesses nacionais e a liberdade de acção no ciberespaço.

[7] Cf. Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a estratégia da UE para a Cibersegurança, Bruxelas, 7.2.2013 – JOIN(2013)

Ao nível operacional está aprovado a criação, instalação e operacionalização de um CNC[8], desenvolvido e coordenado pelo Gabinete Nacional de Segurança (GNS), com a colaboração de todas as entidades relevantes em razão da matéria.

Operacionalizando o termo de cibersegurança à GNR, não há uma estratégia estabelecida para a cibersegurança mas existem uma série de iniciativas que procuram promover boas práticas no que diz respeito à utilização de recursos informáticos.

Ao nível técnico, a segurança da rede interna da GNR procede-se segundo a Figura 2

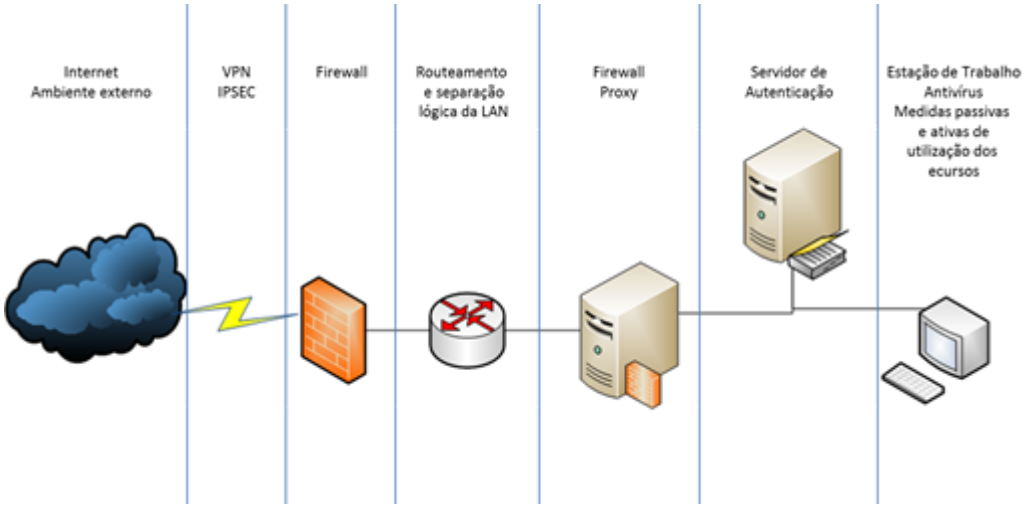


Figura nº 2

Fonte: Raposo, 2013

A segurança da rede é feita ao nível da Segurança Aplicacional e da Segurança de Rede.

São exemplos de procedimentos de Segurança Aplicacional: o controlo e auditoria de acessos, limitação dos utilizadores autorizados, criação de perfis de utilizadores e credenciação dos mesmos e a consciencialização dos termos de responsabilidade civil e criminal.

Como exemplos da Segurança de Rede existem Fire-walls de rede. Equipamentos de Roteamento e separação lógica da LAN[9] e *Fire-walls Proxy*[10]. A Rede é fechada e encriptada, não sendo possível aceder fora destes terminais.

---

[8]Cf. Resolução do Conselho de Ministros n.º 12/2012

[9] *Local Área Network* - Rede de Área Local

[10] Por razões de segurança da rede, os modelos e características dos equipamentos não foram revelados.

4.2.3. Análise à questão n.º 3

No quadro n.º 4, é apresentada a argumentação relativa à **Questão n.º 3 – Qual é o espectro da ameaça no Ciberespaço e quais os principais desafios que coloca às Forças e Serviços de Segurança e à GNR em particular?**

Quadro nº 4

Entrevistado	Ideias Chave
1	- A ameaça pode variar consoante os seus objectivos dos actores e o alvo escolhido. - Uma ameaça transversal a todas as instituições é designada como o *Insider*, utilizadores que não são espectáveis de constituir uma ameaça, que por diversas razões exploram as vulnerabilidades do sistema a partir de dentro do sistema. Em termos de protecção estes elementos não têm problemas em ultrapassar a barreira de segurança física das instalações dado que trabalham no mesmo local mas tem de ultrapassar todas as outras medidas de segurança como o controlo ou credenciação do acesso a essas áreas ou dos terminais de acesso
2	- Não é entendido como ameaça mas como uma fonte de vulnerabilidades é o facto de ser inevitável que os militares utilizem os computadores de serviço para fins pessoais. - O facto das nossas máquinas terem portas de USB[11] abertas que advém do facto da necessidade dos militares muitas vezes trazerem o trabalho feito de casa ou fora de horas. Pois nós ainda não temos uma

11 USB - Universal Serial Bus, é um tipo de conexão de periféricos a aparelhos electrónicos.

	solução segura que nos permita estar a trabalhar em casa e fazer essa transmissão para os terminais sem recorrer a *Pen-Drives*[12]. - Este tipo de comportamentos, na sua maioria não tem intenções danosas, acontecem pela falta de um processo de aculturação desta realidade tecnológica.
3	- As ameaças que advém do ciberespaço variam consoante os agentes, podendo eles ser indivíduos, organizações ou estados, e a sua vontade ou objectivos designadamente a motivação pessoal, o ganho financeiro, a motivação política, ideológica ou religiosa e por fim a vantagem competitiva sobre outro Estado. - Estabelece-se então como as principais ameaças: o cibercrime, o hactivismo, o ciberterrorismo e por fim a ciberguerra.
4	A Rede Nacional de Segurança Interna (RNSI) tem uma ferramenta que detecta os ataques feitos à rede e gera relatórios das ameaças ao sistema. Esta ferramenta só detecta os ataques que estejam sinalizados na base de dados da ferramenta como agentes maliciosos, ou seja ataques novos podem não ser detectados e nós não sabemos os seus efeitos a não ser através dos danos produzidos.

Análise da questão n.º 3

As Ameaças que advém do Ciberespaço variam consoante os agentes, e a sua vontade ou objectivos- Estabelecem-se então como as principais ameaças: o cibercrime, o hactivismo, o ciberterrorismo e por fim a ciberguerra (ver Figura 3)

O principal desafio a nível do Estado é a aplicação de medidas que garanta, a resiliência do ciberespaço, desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da PCSD, desenvolver os recursos industriais e tecnológicos para a cibersegurança.

O principal desafio para a GNR é a aposta num modelo policial nesta área que é o *Cyber-Policing* que prima pela consciencialização das pessoas, empresas e outras

[12] *Pen-Drive* ou Memória USB *Flash Drive* é um dispositivo de memória constituído por memória flash, com uma entrada USB e capacidades de armazenamento variadas.

entidades para estas questões da cibersegurança. Trabalhar numa perspectiva de aconselhamento, prevenção e consciencialização da responsabilidade partilhada que é a cibersegurança.

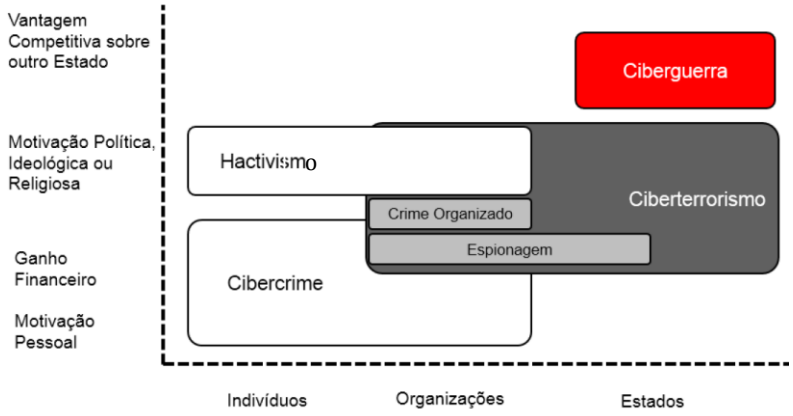


Figura nº 3 Fonte: Santos, 2011

4.2.4. Análise à questão n.º 4

No quadro n.º 5, é apresentada a argumentação relativa à **Questão n.º 4 - Qual o impacto das Ciberameaças na actividade da GNR?**

Quadro nº 5

Entrevistado	Ideias Chave
1	- Não prevejo nenhuma situação em que na eventualidade da ocorrência da paralisação dos sistemas de informação que qualquer actividade operacional da Guarda cesse. É previsível que haja uma redução significativa capacidade de resposta alguns sectores, principalmente onde estes sistemas estão mais implementados como no caso levantamento de autos no trânsito que está totalmente informatizado. O objectivo destes sistemas é agilizar todos os processos burocráticos no momento da fiscalização esta iria ser claramente mais morosa.

2	Tem-se detectado algumas ameaças internas mas não intencionais, alguma curiosidade, não são críticas no sentido de extrair ou danificar informação mas sim de bloqueio ou negação de serviços. Considero os nossos sistemas seguros mas podiam ser ainda mais. Tivemos o exemplo da Polícia de Segurança Pública (PSP) que foi atacada, não na sua rede mas através de um elemento pertencente a uma associação sindical que armazenava dados pessoais dos seus associados no seu computador pessoal. Estando esta base de dados fora da rede da PSP e RNSI, constituía uma vulnerabilidade que o adversário explorou para ter acesso a informação privilegiada.
3	A Guarda não iria parar., mas afectando os seus Sistemas de Informação iria tornar a capacidade de gestão e tratamento da informação um processo mais moroso. Estes Sistemas ajudam os comandantes a tomar decisões de forma mais informada e oportunamente.
4	- Este impacto tem de ser medido a partir das potenciais ameaças e do levantamento dos mecanismos existentes para os proteger . - Existe a necessidade de um levantamento dos activos críticos e quais os meios para os proteger.

Análise da questão n.º 4

Para avaliar o Impacto das actuais Ciberameaças é necessário primeiramente fazer um levantamento dos activos existentes na Guarda, as infra-estruturas críticas, e quais os meios e formas disponíveis para os proteger. Estudados estes elementos poderemos então avaliar o risco e criar Modelos de Gestão de Risco e actuação perante estas Ciberameaças.
Presentemente, após analisado o ambiente internacional, afigura-se que estas ameaças se concretizem por ataques individuais com o objectivo de alterar o conteúdo de páginas de sítios de referência e ataques do tipo *Denial of Service.*

4.2.5. Análise à questão n.º 5

No quadro n.º 6 é apresentada a argumentação relativa à **Questão n.º 5 Que alterações ou ajustamentos serão necessários realizar na GNR para garantir uma**

maior eficácia de actuação no desempenho da sua missão em prol da Cibersegurança e da segurança das Estruturas Críticas Nacionais?

Quadro nº 6

Entrevistado	Ideias Chave
1	- A GNR tem de se preparar para se defender a si própria e os seus sistemas. Cada vez mais caminhamos no sentido nos apoiarmos nas Tecnologias da Informação, como por exemplo o processo de decisão e comunicação. - Aproveitar as nossas capacidades como força de segurança de cariz militar. - Reconhecimento técnico por parte das entidades competentes
2	- Os sistemas homólogos ao da GNR são constituídos por duas componentes, uma administrativa e uma dedicada à segurança, esta última não esta ainda em funcionamento. - Aprovação de Normas de Utilização de Recursos Informáticos. - Melhoramento das componentes físicas dos sistemas de forma a tornar os serviços actuais mais acessíveis e rápidos proporcionando melhor qualidade de serviço. - Estas novas tecnologias permitem mostrar uma imagem da guarda de inovação e profissionalismo que deve ser aproveitada e explorada.
3	-A aposta num modelo policial nesta área que é o *Cyber-Policing* que prima pela consciencialização das pessoas, empresas e outras entidades para estas questões, trabalhando numa perspectiva de aconselhamento, prevenção e consciencialização da responsabilidade partilhada que é a cibersegurança. - Definição e padronização dos conceitos e doutrina para a Guarda e a nível nacional para que todos os elementos utilizem a mesma linguagem. - Propostas de constituição de uma CSIRT da GNR
4	- A criação de uma equipa de resposta a incidentes e a criação de uma outra equipa de recolha de prova digital forense. - A GNR pode actuar face ao Cibercrime no que diz respeito às medidas cautelares e de polícia, sendo necessário que, no decorrer da actividade operacional, surja uma situação de necessidade ou oportunidade.

Análise da questão n.º 5

Segundo os entrevistados, existem já várias iniciativas com o objectivo de responder aos desafios da Cibersegurança que seguem os princípios estabelecidos pela ENISA e pela ENC. No entanto todos defendem que esta área está em constante evolução e desenvolvimento, por conseguinte deveria ser constituído um centro de excelência ou grupo de trabalho o que se dedique permanentemente à investigação, actualização e formação nesta área.

Na área da consciencialização e Formação também surgiram várias iniciativas como as Palestras dos Programas Especiais: Escola Segura sobre "Comunicar em segurança - segurança na Internet" e "*Cyberbullying*". A nível interno, existe uma proposta de um Regulamento de Utilização dos Recursos Informáticos da GNR[13] que no futuro será entregue aos militares que integram os quadros da Guarda Nacional Republicana.

Existe também uma corrente de pensamento que afirma que a Guarda deve primar por ser inovadora e implementar um novo modelo policial nesta área que é o *Cyber-Policing* que prima pela consciencialização das pessoas, empresas e outras entidades para estas questões da cibersegurança.

Relativamente à área da Resposta a Incidentes deveria ser equacionada a criação de uma Célula de Cibersegurança - CSIRT da GNR. No que diz respeito ao combate ao Cibercrime, este é regulado por um grande leque de diplomas legais. Neste contexto, importa simplificar e optimizar legislação para que a sua aplicação seja mais adequada à multiplicidade de situações criminais que por vezes são concorrentes entre si, as quais exigem intervenções mais oportunas por parte de autoridades judiciárias e das FSS.

A aposta na formação poderá abrir portas no sentido de adquirir as competências necessárias para a Guarda coadjuvar o poder político, órgãos ou entidades que tenham responsabilidades nesta área da segurança das Infra-Estruturas Críticas, participando de forma activa na elaboração das políticas de governança do ciberespaço.

[13] Considerando que o Regulamento ainda não foi aprovado e ainda pode ser sujeito a alterações apenas apresento o Índice no Apêndice 1.

Participar no programa nacional de protecção de Infra-Estruturas Criticas, assegurando a representação da Guarda nos diversos fóruns do nosso país. O referido programa tem como objectivos principais identificar, classificar e caracterizar as infra-estruturas críticas existentes em Portugal.

4.3. A Cibersegurança, o Cibercrime e o Normativo Legal Português.

Como vimos anteriormente, a visão estratégica da UE para promover a Cibersegurança articula-se em cinco prioridades, sendo uma delas reduzir drasticamente a cibercriminalidade

Quanto mais as nossas vidas assentam no mundo digital, mais são as oportunidades a explorar pelos cibercriminosos. A cibercriminalidade é uma das formas de criminalidade que mais têm aumentado, fazendo mais de um milhão de vítimas por dia em todo o mundo. Os cibercriminosos e as redes de cibercriminalidade estão a tornar-se cada vez mais sofisticados, pelo que precisamos de dispor das ferramentas operacionais corretas e de capacidades para os combater. Os cibercrimes são altamente lucrativos e de baixo risco e muitas vezes os criminosos exploram o anonimato dos domínios dos sítios Web. A cibercriminalidade não conhece fronteiras, graças ao alcance planetário da Internet, as autoridades policiais devem adoptar uma abordagem transfronteiriça coordenada e de colaboração para responder a esta ameaça crescente. (Comissão Das Comunidades Europeias, 2013)

A UE e os Estados-Membros devem dotar-se de uma legislação rigorosa e eficaz para combater a cibercriminalidade, pois o sistema judicial tem como objectivo principal a dissuasão da prática de crimes, pela prevenção geral (actos de prevenção criminal e o "exemplo" dado pela retribuição social através da sanção penal) e pela especial (a condenação concreta do autor de um crime). A maior parte dos ciberataques configuram ilícitos à luz da legislação nacional e internacional, pelo que importa identificar e julgar os perpetores (Lima, 2009).

Considerando a importância da protecção das Infra-Estruturas Críticas nacionais, o legislador entendeu, através da nova Lei do Cibercrime (LC), alavancar esse princípio dissuasor, agravando consideravelmente as penas aplicáveis a quem realizar ciberataques contra estas (prevenção geral positiva). A título de exemplo, isto significa que numa visão juridicamente pragmática, os crimes informáticos são especiais em relação aos praticados

por meio de tecnologias de informação, processamento e comunicação, dirigindo-se, tendencialmente, contra as pessoas (como exemplo: a pornografia de menores e os crimes contra a honra) ou contra interesses patrimoniais (ex.: direitos de autor, burla informática) ou, finalmente, contra dados e informação (falsidade informática, dano informático, sabotagem informática, acesso ilegítimo, acesso indevido). Só estes últimos constituem crime informático e só estes tipos do crime são totalmente compatíveis com os princípios da segurança informática (confidencialidade, integridade e disponibilidade). Até ao momento, o enfoque nacional quanto à efectivação do princípio da disponibilidade tem encontrado correspondência prática na tentativa de identificação e no planeamento da manutenção das chamadas Infra-Estruturas Críticas nacionais perante desastres (Bravo, 2010).

Como consequência deste tipo de análise em termos de estratégia nacional, deveriam corresponder-lhe como preocupação de âmbito alargado, tanto a manutenção e salvaguarda das referidas Infra-Estruturas Críticas, como uma relativa à manutenção e salvaguarda dos "dados críticos de interesse nacional" (Nunes e Fernando 2010).

A competência legal para prevenção criminal e a investigação criminal dos crimes informáticos está atribuída por lei à PJ, em matéria de informações tendentes a contrariar ou a "garantir a segurança interna e necessárias a prevenir a sabotagem, o terrorismo, a espionagem e a prática de actos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido" a competência é do SIS.[14]

Chegando a investigação a alguma fase de condução de meios de obtenção de prova, com ou sem necessidade de cooperação internacional (policial ou judicial) segue-se o processo penal "clássico" A final deste processo, os resultados obtidos da investigação podem e devem reverter em nova informação, com destino à prevenção criminal e /ou "*intelligence*" (Bravo, 2010).

4.3.1. Lei do Cibercrime

A Lei n.º 109/2009, de 15 de Outubro, estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria

[14] C.f. Lei n.º 49/2008, de 27 de Agosto, LOIC

penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, Convenção de Budapeste (Venâncio, 2006).

Na perspectiva judiciária e policial, a vertente processual desta lei merece ter reforçada atenção, uma vez que o seu âmbito de aplicação exorbita em muito a chamada criminalidade informática. Por força das alíneas b) e c) do respectivo Artigo 11º, as suas disposições processuais são aplicáveis à investigação de muitos outros crimes. Assim sucede com todos os crimes que tenham sido cometidos por meio de um sistema informático ou ainda de todos aqueles em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico – com excepção das intercepções de comunicações e das acções encobertas, Artigos 18º e 19º (Verdelho, 2010).

A principal doutrina portuguesa distingue entre quatro grupos a criminalidade relacionada com a utilização de computadores e em especial na internet:

1.- Os crimes que recorrem a meios informáticos, não alterando o tipo penal comum, correspondem a uma especificação ou qualificação deste, sendo exemplo a devassa por meio de informática (Art.º 193º do CP), o crime de burla informática e o crime de burla informática nas telecomunicações (Art.º 221º);

2.- Os crimes relativos à protecção de dados pessoais ou da privacidade (Lei n.º 67/98, de 26 de Outubro, transposição da Directiva n.º 95/46/CE e a Lei n.º 69/98, de 28 de Outubro);

3.- Os crimes informáticos em sentido estrito, sendo o bem ou meio informático o elemento próprio do tipo de crime. Estes crimes são praticados contra e através do computador, sendo este o alvo da actividade criminosa, inserindo-se aqui os crimes previstos na LC.

4.- No último grupo temos os crimes relacionados com o conteúdo, onde se destacam a violação do direito de autor, a difusão de pornografia infantil (Art.º 172º, n.º 3, alínea d)) ou a discriminação racial ou religiosa (Art.º 240º, n.º 1, alínea a)).

Face ao que antecede, apesar das normas processuais da LC estarem previstas num diploma próprio, aquelas são também aplicáveis a um grande número de processos cujo teor central extravasa o crime informático per si (Dias, 2010).

4.3.2. Competência dos Órgãos de Polícia Criminal face à lei do Cibercrime

Nos termos da alínea l), do n.º 3, do artigo 7.º, LOIC, é da competência reservada da PJ a investigação dos crimes informáticos e praticados com recurso a tecnologia informática. Importa portanto, analisar a competência dos restantes OPC para investigarem os crimes previstos na LC, face ao disposto na referida alínea.

Tendo presente o teor da competência dos OPC, importa examinar, com mais detalhe, o regime definido para a pesquisa de dados informáticos, medida prevista no artigo 15º e para a apreensão de dados informáticos, contemplada no artigo 16º da LC.

A essência destas medidas processuais coincide, no ambiente do ciberespaço, com as formas clássicas de busca e apreensão desenhadas nos artigos 174.º e 178.º do CP **(**Verdelho, 2010).

A pesquisa de dados informáticos num sistema informático conserva a sua verdadeira natureza processual de busca, acrescentando ainda "Apesar da originalidade terminológica da LC, continuam a valer os cânones estabelecidos no Art.º 174º, n.º 1, do CPP, pelo que:

a) Quando houver indícios de que dados informáticos relacionados com um crime ou que possam servir de prova se encontram num determinado sistema informático é ordenada a busca informática;

b) A busca informática é ordenada por despacho pela autoridade judiciária competente, devendo esta, sempre que possível, presidir à diligência" (Mesquita, 2012).

Relativamente à apreensão de dados informáticos, também "não se alteram, os pressupostos funcionais da apreensão em processo penal (cf. Art.º 178º, n.ºs 1 e 3, do CPP), pelo que:

a) São apreendidos os sistemas informáticos e os dados informáticos que tiverem servido ou estivessem destinados a servir a prática de um crime, e bem assim todos aqueles que tiverem sido deixados pelo agente no local do crime ou quaisquer outros susceptíveis de servir de prova;

b) As apreensões de sistemas e dados informáticos são autorizadas, ordenadas ou validadas por despacho da autoridade judiciária."

À semelhança do previsto no n.º 4 do Artigo 178.º do CPP, a LC permite também que o órgão de polícia criminal efectue apreensões, sem prévia autorização da autoridade

judiciária, no decurso de pesquisa informática a um sistema informático legitimamente ordenada, bem como quando haja urgência ou perigo na demora, conforme estabelecido no n.º 2 do Artigo 16.º. As apreensões efetuadas nestas circunstâncias são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas (n.º 4 do mesmo preceito).

A direcção do inquérito cabe ao Ministério Público, assistido pelos órgãos de polícia criminal, conforme se dispõe no n.º 1 do Artigo 263.º, do CPP. Neste âmbito, os OPC atuam sob a directa orientação do Ministério Público e na sua dependência funcional (n.º 2 do mesmo preceito).

Por outro lado, no artigo 2.º da LOIC, relativo à direcção da investigação criminal, proclama-se o princípio segundo o qual a direcção da investigação cabe à autoridade judiciária competente em cada fase do processo, preceituando o n.º 3 que os órgãos de polícia criminal, logo que tomem conhecimento de qualquer crime, comunicam o facto ao Ministério Público no mais curto prazo, sem prejuízo da prática dos actos cautelares necessários e urgentes para assegurar os meios de prova (Dias, 2010).

Da conjugação de todas estas regras, é entendimento que a GNR, enquanto OPC:

1. Tem competências para efectuar a pesquisa e apreensão de dados informáticos, de forma a assegurar os meios de prova decorrentes do cumprimento de actos processuais devidamente ordenados por autoridade judiciária competente;

2. Com instruções da autoridade judiciária, pode efectuar a pesquisa e apreensão de dados informáticos em crimes conexos, cuja tipologia não tenha a característica de crime informático, nem o objecto central do crime seja atingido recorrendo ao computador;

3. Se tiver qualquer conhecimento de factos tipificados como crimes, também no âmbito da LC, ou cuja investigação se encontra legalmente reservada à PJ, e sem prejuízo dos casos de competência deferida previstos no Art.º 8º da LOIC, deve a Guarda promover os actos cautelares necessários e urgentes para assegurar os meios de prova e remeter, com conhecimento à autoridade judiciária, o processo para o órgão de polícia criminal competente, no mais curto prazo.

Face ao que antecede, é entendimento que, para efectuar a apreensão e pesquisa de dados informáticos, e para promover actos cautelares necessários e urgentes, a GNR necessita de possuir conhecimentos, capacidade tecnológica e recursos humanos, integrados numa estrutura que a habilite a tal desiderato.

Capítulo 5
Conclusões

5.1. Verificação das Hipóteses Enunciadas

Estaremos agora em condições e com o fundamento necessário, responder às interrogações que surgiram no nosso raciocínio desde a fase mais embrionária da concepção deste trabalho. Assim, procuraremos determinar a veracidade daqueles que foram os pressupostos que guiaram a nossa investigação ao longo da sua fase mais empírica.

"H1 – O Ciberespaço tem cada vez mais importância na actualidade."

Esta Hipótese é validada pois verifica-se que nas últimas duas décadas, a Internet e o ciberespaço tiveram um impacto enorme em todos os sectores da sociedade, e estão relacionados com todos os aspectos da vivência na era da Informação. Fazendo uma análise abrangente, neste momento, a nossa sociedade e o Ciberespaço são duas realidades indissociáveis.

A nossa vida diária, os direitos fundamentais, as interacções sociais e as economias dependem continuamente do funcionamento das tecnologias da informação e das comunicações. Um ciberespaço aberto e livre tem promovido a inclusão política e social em todo o mundo; derrubando as barreiras entre países, comunidades e cidadãos, permitindo a interacção e a partilha de informações e ideias entre todos os pontos do mundo; proporcionou um fórum para a liberdade de expressão e o exercício dos direitos fundamentais e deu às pessoas meios para lutarem por sociedades democráticas e mais justas como a primavera árabe demonstrou de modo impressionante.

"H2 – O Ciberespaço acarreta responsabilidades de segurança para o Estado e as suas Forças de Segurança."

Esta Hipótese é validada. O Ciberespaço é uma realidade e um fenómeno muito mais complexo e abrangente do que a Internet propriamente dita, compreendendo serviços, modelos de negócio, infra-estruturas, diferentes dinâmicas sociais próprias, bem como diferentes tipos de atores (ex.: cidadãos, empresas, organizações, estados, etc.).

Ainda neste contexto, é consensual que actualmente o Ciberespaço é a 5ª dimensão de um teatro de operações que compreende as já 4 dimensões até ao momento existentes: a terra, o mar, o ar e o espaço.

Cumulativamente o ciberespaço, é extremamente predisponente a todo o género de práticas criminais, belicistas e subversivas. Isto verifica-se pelo facto das comunicações se processarem a nível planetário entre uma rede infindável de dispositivos tecnológicos e interdependentes, em que se considera faltar o elemento territorialidade para se poder impor o direito nacional e internacional.

Acresce o facto de ser difícil reconstituir qualquer percurso criminal entre os diferentes agentes delituosos, em virtude dos actos serem praticados em diversos pontos do ciberespaço, sentindo-se os infractores protegidos pelo anonimato que esta rede lhes proporciona; Este facto tem repercussões ao nível da segurança pois "O Ciberespaço é o estado tecnológico mais aproximado da natureza humana". As condutas criminosas praticadas no mundo real, estão a ser praticadas de forma homóloga no Ciberespaço e cada vez mais, esta tipologia de crimes torna-se mais organizada, complexa e tecnologicamente avançada.

Neste âmbito, as ameaças existentes no ciberespaço não devem ser só encaradas numa perspectiva regional mas numa dimensão holística a qual compreende todas as áreas do conhecimento humano.

Neste quadro, o actual espectro de ameaças existentes no Ciberespaço, tendo em consideração a motivação e o perfil dos seus autores, pode ser caracterizado por meras incivilidades, acções de hactivismo, cibercrime, espionagem, ciberterrorismo e por ciberguerra.

"H3 – Portugal tem uma Estratégia de Cibersegurança capaz de garantir a segurança das Estruturas Críticas."

Esta Hipótese encontra-se refutada no sentido estrito dado que Portugal ainda não tem uma Estratégia de Cibersegurança aprovada, no entanto existe uma proposta elaborada pelo GNS. Foi aprovado também em Resolução de Conselho de Ministros n.º 12/2012 o qual visa a implementação de uma estratégia global da Administração Pública na área das Tecnologias de Informação e Comunicação apresentada pelo Grupo de Projecto para as Tecnologias de Informação e Comunicação instituído pela Resolução do Conselho de

Ministros n.º 46/2011, de 14 de Novembro, de forma a consolidar a Estratégia Nacional de Segurança da Informação, sendo que esta compreende a criação do CNC.

"H4 – As Infra-Estruturas Críticas da GNR são seguras."

Esta Hipótese foi parcialmente verificada pois segundo os testemunhos até ao momento ainda não foi relatada nenhuma intrusão nas infra-estruturas críticas da GNR. Apesar de ainda não existir uma CSIRT própria da GNR, a monotorização da sua rede é feita pela Repartição de Redes e Sistemas de Apoio. Estes sistemas sofreram recentemente um *upgrad*e de forma a possibilitar uma maior disponibilidade, velocidade e segurança na resposta de pedidos. Ao nível técnico, a segurança da rede interna da GNR procede-se segundo a Figura 2. Existem outras iniciativas de forma a implementar um rol de boas práticas com o intuito de fomentar a cultura da Cibersegurança na Instituição. Fica ressalvado no entanto, dado que nenhum sistema é impenetrável, pese embora a ínfima probabilidade, a ocorrência de uma intrusão que não fosse relatada pelas ferramentas de monotorização da rede, pela elevada complexidade ou por ser tão inovador que não fosse reconhecido como ameaça.

"H5 – A GNR mantêm o seu nível de Operacionalidade no caso de ser alvo de um ataque às suas Infra-Estruturas Críticas.

Esta Hipótese é verificada dado que existem processos redundantes na execução de toda a actividade operacional da GNR. É de salientar que no entanto a capacidade administrativa e logística irá ser reduzida.

"H6 – Os Modelos de Actuação da GNR satisfazem as necessidades de Cibersegurança da sua competência."

A Hipótese é parcialmente comprovada. Dado que segundo os entrevistados, existem já várias iniciativas com o objectivo responder às necessidades da Cibersegurança. No entanto todos defendem que esta área está em constante evolução e desenvolvimento, por conseguinte deveria ser constituído um centro de excelência ou grupo de trabalho o que se dedique permanentemente à investigação, actualização e formação nesta área.

Existe também uma corrente de pensamento que afirma que a Guarda deve primar por ser inovadora e implementar um novo modelo policial nesta área que é o Cyber-Policing. Este modelo coloca em primeiro plano a consciencialização das pessoas, empresas e outras entidades, tendo em vista as questões da cibersegurança.

5.2. Reflexões Finais

No decorrer da elaboração do trabalho foi constatado que a Cibersegurança será uma das principais preocupações dos Estados neste século, em particular no que diz respeito à segurança das Infra-Estruturas Críticas de Informação. Na fase do trabalho foi possível conhecer a vertente da Cibersegurança da Guarda e pelos testemunhos recolhidos e análise da legislação prevê-se também que será exigido à GNR adaptar-se a esta nova realidade.

Esta adaptação deve ser orientada por em seis objectivos, sendo eles: a investigação e desenvolvimento, normalização e certificação, formação e consciencialização, alerta e resposta a incidentes, combate ao cibercrime e protecção de infra-estruturas críticas.

No que diz respeito à investigação e desenvolvimento a Guarda, através dos seus centros de formação deveria ser constituida doutrina e a promoção de iniciativas de investigação e de desenvolvimento nas áreas de investigação criminal do meio digital com base na sua experiência policial. Neste contexto, deveriam também estabelecer-se relações privilegiadas com o CNC nestas áreas. Cumulativamente, o sucesso da investigação no meio digital depende também da formação e do treino conjunto com outros atores, nomeadamente as autoridades judiciárias, advogados e restantes operadores jurídicos e funcionários. Seguidamente torna-se necessário o reforço do investimento público no sentido de promover parcerias entre as instituições de ensino, sector público e privado, ou com as instituições com responsabilidades no domínio da segurança no que diz respeito à protecção de Infra-Estruturas Críticas.

O sector da Normalização e Certificação é fundamental na área da segurança informática, especialmente num contexto de adopção de futuras estratégias de cibersegurança na EU. É necessário existirem normas e boas práticas internacionalmente reconhecidas por forma a facilitar a comunicação e a cooperação entre os diversos atores ao nível internacional, sejam eles entidades privadas ou Estados.

Neste âmbito já existem organizações nacionais e internacionais que produzem normas relacionadas com o ciberespaço. Na Europa esses grupos de trabalho são promovidos pela ENISA.

Em Portugal, o papel de promover a criação e a coordenação de esforços nos grupos de trabalho, que podem ser constituídos nas diversas entidades ou organizações, com o objectivo de elaborar documentação de "boas práticas" ou regulamentação adequada às suas realidades específicas, poderia ser confiado ao CNC

Relativamente ao eixo Formação e Consciencialização é necessário ter-se em consideração que a cibersegurança não é uma responsabilidade exclusiva do Estado, mas sim, uma responsabilidade partilhada com outros atores nomeadamente o sector público-privado, as organizações e os cidadãos.

No âmbito da consciencialização do sector público-privado, bem como dos cidadãos, as entidades com responsabilidade na área da segurança poderiam planear e conduzir programas especiais de consciencialização relativamente às ameaças que podem advir do ciberespaço.

Relativamente aos Alertas e Resposta a Incidentes, tendo em consideração esta necessidade em se assegurar um sistema de alerta e resposta a incidentes, surgiram, no contexto da cibersegurança, os chamados CSIRT, no sentido de se fomentar uma melhor cooperação internacional e troca de informações. Neste contexto é essencial a existência, ao nível nacional de um ponto de contacto ou um CSIRT único, ao qual caberia coordenar a actividade de outros CSIRT's em áreas diversas do sector público ou privado.

No caso particular do eixo Combate ao Cibercrime, no que diz respeito à prova digital é necessário frisar-se que a mesma tem um carácter temporário e de grande volatilidade, pelo que a sua recolha e preservação torna-se complexa e difícil de garantir no que diz respeito à validade da custódia da prova em sede de juízo. Assim sendo, existem alguns desideratos, nomeadamente ao nível da sua: admissibilidade, autenticidade, precisão e completude.

Importa referir que ao nível nacional o Cibercrime está regulado por um grande leque de diplomas legais. Neste contexto, importa simplificar a legislação para que a sua aplicação seja mais adequada à multiplicidade de situações criminais que por vezes são concorrentes entre si, as quais exigem intervenções mais oportunas por parte de autoridades judiciárias e das FFSS;

Ainda relativamente à recolha da prova digital associada ao Cibercrime é necessário a alocação de recursos tecnológicos *High-Tech* às FFSS, formando recursos humanos com a necessária *expertise*, capacitando-as no domínio de conhecimentos científicos, técnicos e forenses por forma a prevenir e combater este flagelo. Por outro lado é necessário garantir-se a efectiva operacionalização do CNC, o qual irá permitir a coordenação e a resposta nacional a ciberameaças com a missão de assegurar também acções de cooperação ao nível internacional. Considera-se que este centro é absolutamente estratégico para operacionalizar uma política nacional de combate às Ciberameaças.

No que diz respeito à Protecção de Infra-Estruturas Críticas, é necessário definir com exactidão o que se considera uma Infra-Estrutura Crítica, tendo em vista estabelecer, no plano operacional, regras de empenhamento ao nível das organizações internacionais e ao nível dos Estados. Após a definição clara destes conceitos é necessário proceder-se à efectiva identificação e classificação de Infra-Estruturas Críticas existentes nos diferentes Estados e dentro da Guarda. Isto implica a identificação de sectores críticos e a valoração dos seus activos.

5.3. Recomendações

Face aos resultados apresentados e às conclusões tomadas foi apontada a necessidade da criação um grupo de trabalho multidisciplinar, tendo em vista planear a futura participação da GNR na ENSI. Assim a Guarda deve consciencializar a tutela, no âmbito da ENSI, no sentido de serem criadas as condições necessárias para contribuir mais activamente na operacionalização efectiva do CNC de harmonia com a medida 4 da Resolução n.º 12/2012 da Presidência do Conselho de Ministros Português. Ainda neste âmbito, deveria encetar-se esforços no sentido de fazer-se representar, no âmbito das suas competências, nesse CNC através de recursos humanos qualificados.

Sob a coordenação do Comando de Doutrina e Formação, recorrendo à *expertise* da Direcção de Informações (DI), Direcção de Investigação Criminal (DIC) e Direcção de Comunicações e Sistemas de Informação (DCSI), planear-se a criação de um próprio CSIRT à imagem e semelhança de já existentes em outros sectores nacionais. Este CSIRT deve ser chefiado pela DCSI e encontrar-se sob a dependência funcional da DIC ou da DI. A GNR deve planear e garantir a formação especializada de recursos humanos, em

áreas específicas de investigação policial do meio digital, tendo em vista poder, no futuro, integrar um possível ”Laboratório Forense Único” no âmbito do meio digital, apesar de essa competência ser agora exclusiva da PJ. Neste contexto estudar a viabilização do alargamento de competências de investigação do meio digital para a GNR. A Guarda neste contexto tem a vantagem de se encontrar implantada em todo o território nacional, facto que lhe poderá permitir reunir condições únicas para investigar incidentes em todas as infra-estruturas críticas distribuídas por pzortugal.

Deverão ainda ser estabelecidos contactos com as Forças Armadas no sentido da GNR poder participar de forma mais activa em programas e fóruns que se realizem no âmbito da ENSI e paralelamente, se estabeleçam contactos e se estreitem relações de maior proximidade com a nova unidade especial de combate á cibercriminalidade recentemente criada pela INTERPOL, bem como com a EUROPOL, definindo com mais precisão a sua participação na prevenção e no combate a estes flagelos.

Por fim, sendo sobejamente previsível, por aquilo que já foi referido que, no futuro, ocorram incidentes que atentem contra a cibersegurança do nosso país, propõe-se que a GNR, sob a direcção da Direcção de Operações, apoiada pela DI, DIC e DCSI promova a criação de “programas especiais de polícia” ligados ao *Cyber-Policing*, tendo em vista a consciencialização dos cidadãos e de outros sectores público-privados sobre as diversas formas que existem para minimizar os seus efeitos.

5.4. Limitações

Devemos apenas referir, que devido à especificidade técnica do tema escolhido, surgiram certas dificuldades na realização do trabalho especialmente na compreensão das estruturas de segurança dos Sistemas.
Por outro lado, a criticidade do objecto de estudo não permitiu que este aprofundasse os certos objectivos de investigação.

Referências Bibliográficas

Arquilla, J. and D. Ronfeldt (Eds.) (2001). *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica, CA: Rand Corporation. em Julho de 2008.

Ascenção, J. O. (2000). *Direito da Sociedade da Informação, Vol. II, Chapter - Criminalidade Informática*. Coimbra: Coimbra Editores.

Bardin, L. (2008). *Análise de conteúdo* (4.ª Ed.). Lisboa: Edições 70

Bell, D. (2001). *An introduction to cybercultures*. London: Routledge

Bravo, R. (2006). *Tráfico, branqueamento e terrorismo: a relevância das TIC's*, Lisboa: ADT da Polícia Judiciária.

Bravo, R. & Luís, F (2008). *Cyberterrorismo e informação digital: da contenção de ataques nas redes de informação, à catalogação por grupos de autores*, Lisboa: SCICAT. Direcção Central de Investigação da Corrupção e Criminalidade Económica e Financeira - DCICCEF. PJ.

Bravo, R. (2010). *Do espectro de conflitualidade nas redes de informação: por uma reconstrução conceptual do terrorismo no ciberespaço*, Polícia Judiciária

Brechbühl, H., R. Bruce, S. Dynes, and M. E. Johnson (2010), *"Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*", Information Technology for Development 16 (1), pp. 83 – 91.

Broadhurst, R. and Chantler, N. (2006). *Cybercrime Update: Trends and Developments. Technical report*, Expert Group Meeting on the Virtual Forum against Cybercrime, In Collaboration with UNODC (United Nations Office on Drugs and Crime)

Carvalho, J. E. (2009). *Metodologia do Trabalho Científico - «Saber-Fazer» da investigação para dissertações e teses* (2.ª ed.). Lisboa: Escolar Editora

Campos, F. M. (2002). *Informação Digital: um novo património a preservar*. Cadernos de Biblioteconomia Arquivística e Documentação Cadernos BAD, (002), 8-14.

Casagrande, D. (1999). *Informantion as Verb: Re-concetualizing Information for Cognitive and Ecological Models.*

Chandler, D and Munday, R (2011) , *A Dictionary of Media and Communication.* Oxford University Press.

Comissão Das Comunidades Europeias. (2012). *Comunicação Da Comissão Ao Parlamento Europeu, Ao Conselho, Ao Comité Económico E Social Europeu E Ao Comité Das Regiões relativa à protecção das infra-estruturas críticas da informação "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência*"

Comissão Das Comunidades Europeias. (2013). *Comunicação Conjunta Ao Parlamento Europeu, Ao Conselho, Ao Comité Económico E Social Europeu E Ao Comité Das Regiões Estratégia da União Europeia para a cibersegurança.*

Comninos, Alex. (2013). A cyber security agenda for civil society: what is at stake?

Coutinho, C. (2011). *Metodologia de investigação em ciências sociais e humanas: teoria e prática.* Coimbra: Almedina.

Couto, C (1988). *Elementos de Estratégia, Apontamentos para um Curso*. Volume I, IAEM, Lisboa.

Cybercrime (2013): *Conceptual Issues for Congress and U.S. Law Enforcement,*

Dias, V (2010). *A Problemática Da Investigação Do Cibercrime*, Universidade De Lisboa

Denning, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy, Chapter Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy*, pp. 239-288. Santa Monica, CA: RAND Corporation.

Kissel, R. (2011). *Glossary of Key Information Security Terms,* National Institute of Science and Technology, U.S. Department of Commerce February.

Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Technical report, Center for Strategic and International Studies.

Libicki, M. C. (1995). *What Is Information Warfare?* Washington, D.C.: United States Government Printing.

Lima, L. (2009) – *"Lei do Crime Ineficaz"*, Almedina.

Floridi, L. (2013). *Semantic Conceptions of Information.* ,The Stanford Encyclopedia of Philosophy

Fenz. (2005). *Cyberspace Security: A definition and a description of remaining problems*

Freire, F. e Nunes, P. (2009). *"Nunca de Antes"*, Anuário do Instituto da Defesa Nacional, 1, 53-59.

Freixo, M. J. V. (2011). *Metodologia Científica* (3.ª ed.). Lisboa: Instituto Piaget.

Gibson, W. (1984). Neuromancer, HarperCollins

Grabosky, P. (2004). *The Global Dimension of Cybercrime*. Global Crime 6 (1),pp. 146-157.

Graham, M. (2011). *Time machines and virtual portals: The spatialities of the digital divide* International Telecommunications, (2008). Union (ITU), *Telecommunications Standardization Sector, Overview of Cyber security, Recommendations*

Marques, A (2012), *Congresso da Justiça*

Martins, L. (2003). *Direito da Sociedade da Informação, Vol. IV, Chapter Criminalidade Informática*. Coimbra: Coimbra Editores.

Mendes, C (2012) ,*Publicação Mensal Da Autoridade Nacional De Protecção Civi* L / N.º 51 / JUNHO. I S SN 16 4 6 – 95 42.

Nunes, P e Fernando, V. (2010). *Mundos Virtuais, Riscos Reais: Fundamentos Para a Definição de Uma Estratégia da Informação Nacional*, ICNSD.

Ottis., Lorents. (2012) *Cyberspace: Definition and Implications*

Pedahzur, A. (2009). *The Israeli Secret Services & the struggle against Terrorism. Nova Iorque,* Columbia University Press.

Ralston, A.(2000) *Encyclopedia of computer science* Nature Pub. Group,

Santos, J. (2011) *Contributos para uma melhor governação da cibersegurança em Portugal.* Faculdade De Direito da Universidade Nova De Lisboa

Santos, L (2000). *Estratégia Militar no Início do Século XXI*. Conferência no IAEM, Dezembro, Lisboa.

Sarmento, M. (2008). *Guia prático sobre a metodologia científica para a elaboração, escrita e apresentação de teses de doutoramento, dissertações de mestrado e trabalhos de investigação aplicada* (2.ª ed.). Lisboa: Universidade Lusíada Editora.

Silva, P. T., Carvalho, H., & Torres, C. B. (2003). *Segurança dos sistemas de informação: gestão estratégica da segurança empresarial*.

Sistema de Segurança Interno, (2012). *Relatório Anual de Segurança Interna*

Sousa, M e Baptista, C. (2011) *Como Fazer Investigação, Dissertações, Tese e Relatórios*, Pactor

Valente, J. (2001). *"Segurança nos Sistemas de informação"*. Dirigir n. º 13. Lisboa: IEFP,.

Venâncio, P. (2006) – *Breve introdução da questão da Investigação e Meios de Prova na Criminalidade Informática*, Verbojuridico, Dezembro,

Verdelho, P (2003) "Cibercrime", Direito da Sociedade da Informação, APDI, volume IV, Coimbra Editora, págs. 347-383.

Verdelho, P. Bravo, R e Rocha, M (coord. e notas) – *Leis do Cibercrime*, volume 1, CentroAtlantico.pt, Portugal, 2003.

Verdelho, P (2005) "Cibercrime e segurança informática", Polícia e Justiça, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III série, nº 6, Julho-Dezembro, Coimbra Editora,

Verdelho, P (2010) "A nova Lei do Cibercrime", Lei nº 109/2009, Boletim da Ordem dos Advogados, nº 65

Martins, L. (2003). *Direito da Sociedade da Informação, Vol. IV, Chapter Criminalidade Informática*. Coimbra: Coimbra Editores.

Mesquita, Paulo (2010) *Processo Penal, Prova e Sistema Judiciário*

Nunes, P e Fernando, V. (2010). *Mundos Virtuais, Riscos Reais: Fundamentos Para a Definição de Uma Estratégia da Informação Nacional*, ICNSD.

Anexo 1

GUIÃO DE ENTREVISTA

Antes do início da entrevista, gostaria de saber se tem alguma dúvida ou questão relativamente à mesma?
Coloca algum entrave quanto à gravação da entrevista e posterior utilização do seu conteúdo no relatório científico final do trabalho de investigação aplicada?

Caraterização do(a) entrevistado(a):

Nome:

Posto:

Função:

Outras informações:
Local: **Data:** **Hora:**

Perguntas:

Pergunta n.º 1: O que é o Ciberespaço e que desafios coloca às modernas sociedades e ao ambiente de segurança?

Pergunta n.º 2: O que é e como é possível garantir a Cibersegurança das Estruturas Críticas Nacionais?

Pergunta n.º 3: Qual é o espectro da ameaça no Ciberespaço e quais os principais desafios que coloca às Forças de Segurança e à GNR em particular?

Pergunta n.º 4: Qual o impacto das Ciberameaças na actividade operacional da GNR?

Pergunta n.º 5: Que alterações/ajustamentos serão necessários realizar na GNR para garantir uma maior eficácia de actuação, no desempenho da sua missão e em prol da Cibersegurança das Estruturas críticas?

Anexo 2

Relatório Síntese da Entrevista ao Sr Major Bessa

Q.1 – O que é o Ciberespaço e que desafios coloca às sociedades modernas e ao ambiente de Informação?

– O ciberespaço é mais do que a Internet, esta surgiu com objectivos militares até que se expandiu para o mundo civil e cada vez mais nós passamos a estar próximos e ter a capacidade de comunicar e partilhar vários tipos de informação.

-O problema da partilha, é que muitas vezes se partilha mais do que queremos, sem nos apercebermos. A partir do momento que temos uma rede global, em que o ciberespaço é um conjunto de nós que nos permite comunicar e interligar-nos, se não tivermos precações para nos protegermos e monitorizarmos aquilo que entra e sai dos nossos equipamentos corremos o risco de expormos mais do que queremos até aquilo que não queremos, até mesmo informações e dados pessoais.

- O ciberespaço é a capacidade de comunicarmos, é tudo o que está publicado na internet, esta já se encontra num patamar de estabelecimento de relações pessoais. Tendo em conta que não sabemos onde é que esta informação é guardada. Sabemos que toda a informação que existe no ciberespaço está guardada num suporte físico

-Tudo aquilo que nós disponibilizamos no ciberespaço já mais conseguimos retirar. Seja uma imagem ou comentário em alguma rede social, pois mesmo que o apaguemos a informação já se propagou pelo ciberespaço e é impossível garantir que ela tenha sido mesmo eliminada.

- Apesar do Ciberespaço ser um conceito abstracto ele materializa-se numa componente física A informação existe fisicamente em algum lado, existem outros equipamentos que asseguram a comunicação e todos estes patamares devem ser salvaguardados. Cada um destes pontos pode constituir vulnerabilidades e quebras de segurança.

Q2 – O que é e como é possível garantir a Cibersegurança das Infra-Estruturas Críticas Nacionais?

Penso foi criado agora recentemente um Centro de Cibersegurança Nacional sobre a alçada do Gabinete Nacional de Segurança. No entanto este centro ainda está numa fase de implementação, sendo que quem está envolvido neste projecto são elementos formados nestas áreas das tecnologias

da informação pertencentes aos diferentes ramos das Forças Armadas. Não existe participação por parte de elementos pertencentes às Forças e Serviços de Segurança sendo que este órgão depende directamente do GNS e este por sua vez da Presidência do Conselho de Ministros. A sua principal função será a prossecução da ciberdefesa e reagir às ameaças e protecção e prevenção permanente.
- Um Sistema Crítico tem que garantir a continuidade do Serviço, isso pode passar pela criação de Sistemas Redundantes.
- Definição de normas de segurança
- A segurança é uma responsabilidade de todos
- Segurança física, controlo de acessos tem de respeitar certos protocolos e aspectos de segurança. Os utilizadores são elementos do Sistema e se não fizer uma utilização instruída e consciente da sua responsabilidade para a segurança, pode ser um dos pontos mais frágil para a segurança

Q 3 – Qual é o espectro da ameaça no Ciberespaço e quais os principais desafios que coloca às Forças e Serviços de Segurança e à GNR em particular?

A ameaça pode variar os seus objectivos, ter acesso à informação que disponível no sistema, retirar essa informação ou mesmo tornar o sistema indisponível.
- Exemplo da linha nacional de assistência 112, um ataque de negação de serviço neste sistema iria negar ou aumentar exponencialmente o tempo de reacção até receber uma chamada. Isso poderá ter implicações graves para o cidadão nomeadamente no accionamento dos meios de socorro em casos de incêndios ou emergências médicas. Se este número não estiver disponível para o cidadão
- A principal fonte de ameaça são os utilizadores internos, que pretendem abusar do sistema, por curiosidade, para demonstrar competências ou por vingança pessoal, procuram, identificam e exploram as fragilidades do sistema.
- São designados os *Insiders* utilizadores que não são espectáveis de constituir uma ameaça, que por diversas razões exploram as vulnerabilidades do sistema a partir de dentro do sistema. Em termos de protecção estes elementos não têm problemas em ultrapassar a barreira de segurança física das instalações dado que trabalham no mesmo local mas tem de ultrapassar todas as outras medidas de segurança como o controlo ou credenciação do acesso a essas áreas ou dos terminais de acesso

Hackers/Hacktivists

Q.4 – Qual o impacto das Ciberameaças na actividade da GNR?

- Garantia da continuidade do serviço.
- E que se mantenha uma ligação segura com os serviços que não estão sob a nossa responsabilidade. Ou seja, quando fizermos uma consulta, esse pedido e a resposta sejam transmitidos de forma segura.
- Relativamente os sistemas de informação da GNR são ferramentas de apoio e suporte à decisão e à actividade operacional, ou seja permitem a quem necessita, ter acesso à informação disponível mais rapidamente. Exemplo prático: a consulta de dados numa acção de fiscalização rodoviária que nos dias de hoje a consulta de alguma informação é praticamente imediata.
- Não prevejo nenhuma situação em que na eventualidade da ocorrência da paralisação dos sistemas de informação que qualquer actividade operacional da Guarda cesse, é claro previsível que haja uma redução significativa de alguns sectores, principalmente onde estes sistemas estão mais implementados como no caso levantamento de autos no trânsito que está totalmente informatizado. É levanta-los em papel mas levariam muito mais tempo a serem realizados. Os objectivos destes sistemas é agilizarem todos os processos burocráticos no momento da fiscalização.

Q.5 Que alterações ou ajustamentos serão necessários realizar na GNR para garantir uma maior eficácia de actuação no desempenho da sua missão em prol da Cibersegurança e da segurança das Estruturas Críticas Nacionais?

- GNR tem de se preparar para se defender a si própria e os seus sistemas. Casa vez mais caminhamos no sentido nos apoiarmos nas Tecnologias da Informação, como por exemplo o processo de decisão e comunicação.
- Um dos passos possíveis seria a criação de uma equipa de monotorização de todo o sistema em permanência e com capacidade de intervenção e eliminação de fragilidades. Minimizar as possibilidades de afectar os sistemas.
- Aproveitar as nossas capacidades como força de segurança de cariz militar. Temos elementos com capacidade técnica
- Reconhecimento técnico por parte das entidades competentes
- Intervencionar sobre a prevenção

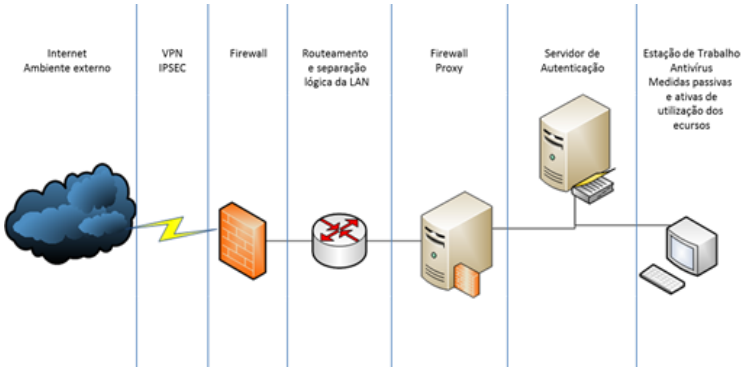
Relatório Síntese da Entrevista ao Sr Capitão Raposo

Q.1 – O que é o Ciberespaço e que desafios coloca às sociedades modernas e ao ambiente de Informação?

- O Ciberespaço é a auto-estrada da comunicação virtual, que liga as pessoas, os sistemas através de nós e redes de comunicação. É um novo espaço de interacção humana que já tem uma importância enorme sobretudo no plano económico e científico e, certamente, essa importância tem concequencias a nível da segurança que o cidadão não pode ignorar

Q2 – O que é e como é possível garantir a Cibersegurança das Infra-Estruturas Críticas Nacionais?

- O conceito de segurança pode ser explicado como o efeito produzido pelo um pingo de água num lago em que os vários círculos constituem os diversos perímetros. Quanto no exterior do círculo estiver menor é o grau de segurança mas também é menor o valor da informação disponível. Quanto mais próximo do centro mais robustas e complexas são as medidas de segurança, e que no centro se encontram as estruturas críticas.
- As nossas estruturas críticas é tudo o que é considerado aplicações centrais, SIOP, SGO, SGRH, SGRL, SGRF.
- São exemplos de procedimentos de segurança: o controlo de acessos, auditoria de acessos, limitação dos utilizadores autorizados, criação de perfis de utilizadores e credenciação dos mesmos, conscientes dos termos de responsabilidade civil e criminal.
- Segurança física como as portas blindadas e anti fogos
- Segurança aplicacional e seg de rede. Fire-walls de rede. Equipamenteos . Rede fechada e encriptada, não sendo possível aceder fora destes terminais. Todos os utilizadores
- Nas aplicações utiliza-se com credenciação, o que permite que todos os acessos internos sejam auditáveis, ou seja, qualquer alteração feita fica associada a um Utilizador podendo este ser responsabilizado pelas suas acções no sistema
- Sendo que é utópico pensar que um sistema é 100% seguro
- Temos de zelar ao máximo pela protecção dos dados, no caso de existir algum incidente repor o mais rapidamente os dados e o sistema.



Q 3 – Qual é o espectro da ameaça no Ciberespaço e quais os principais desafios que coloca às Forças e Serviços de Segurança e à GNR em particular?

- Não é entendido como ameaça mas como uma fonte de vulnerabilidades é o facto de ser inevitável que os militares utilizem os computadores de serviço para fins pessoais. Isto será sempre permitido utilizar o computador para fins pessoais de uma forma a não perturbar o cumprimento do dever de cada militar. Faz sentido é existirem mecanismos ou medidas que impeçam o aparecimento e propagação de ameaças e vulnerabilidades.
- O facto das nossas máquinas terem portas de USB*(explicar USB) abertas que advém do facto da necessidade dos militares muitas vezes trazerem o trabalho feito de casa ou fora de horas. Pois nós ainda não temos uma solução segura que nos permita estar a trabalhar em casa e fazer essa transmissão para os terminais sem recorrer a Pen-Drives.
- Este tipo de comportamentos, na sua maioria não tem intenções danosas, acontecem pela falta de um processo de aculturação desta realidade e tecnologia.
- Um exemplo de uma ameaça concretizada , não com a GNR mas com a PsP, em que houve uma quebra de segurança em que dados pessoais dos agentes inscritos numa associação foram divulgados por parte de uma pessoa externa à instituição.
- Na GNR trabalha-se em duas redes, a nossa, baseada aqui neste centro de dados e na RNSI.
- Esta Rede Nacional de Segurança Interna foi criada de forma a concentrar nela o máximo de serviços comuns e partilhados pelas diversas entidades com o objectivo de centralizar a informação e ao mesmo tempo reduzir custos.
- A análise e tratamento das ameaças é feita Repartição de Aplicação e Sistemas. A reposição de Serviços também pode ser feita pela Divisão dos sistemas de redes

Q.4 – Qual o impacto das Ciberameaças na actividade da GNR?

O que se tem detectado algumas ameaças internas mas não intencionais, alguma curiosidade, não são críticas no sentido de extrair ou danificar informação mas sim de bloqueio ou negação de serviços.
Quando detectamos uma ameaça ou recebemos o alerta, ou tentamos resolver, e caso na consigamos chamamos
Considero os nossos sistemas seguros mas podiam ser ainda mais
Tivemos o exemplo da PSP que foi atacada, não na sua rede mas através de um elemento pertencente a uma associação sindical que armazenava dados pessoais dos seus associados no seu computador pessoal. Estando esta base de dados fora da rede da PSP e RNSI, constituía uma vulnerabilidade que o adversário explorou para ter acesso a informação privilegiada

Q.5 Que alterações ou ajustamentos serão necessários realizar na GNR para garantir uma maior eficácia de actuação no desempenho da sua missão em prol da Cibersegurança e da segurança das Estruturas Críticas Nacionais?

- Deveria existir um grupo especializado e 100% dedicado a esta tarefa, trabalhando de forma proactiva, executar planeamentos de segurança e contingência, resposta a ataques diversos.
- Normalmente nas outras instituições estes sistemas são constituídos por duas componentes uma administrativa em tudo semelhante a esta direcção e uma dedicada à segurança que não existe homóloga na GNR
- Normas de utilização de equipamentos –(ainda não foi aprovado e por isso não é a versão final) (deviam ser aprovadas antes se ser expandida a rede nacional para que seja facultado e distribuído pelo dispositivo)
- Neste momento existe uma aposta muito forte no melhoramento das componentes físicas dos sistemas que nos permitirá tornar os serviços actuais mais acessíveis e rápidos proporcionando melhor qualidade de serviço
- Estas novas tecnologias permitem mostrar uma imagem da guarda de inovação e profissionalismo que deve ser aproveitada e explorada

Relatório Síntese da Entrevista ao Sr Major Santos

Q.1 – O que é o Ciberespaço e que desafios coloca às sociedades modernas e ao ambiente de Informação?

– O ciberspaco conceito mais lato que a Internet, surgiu com âmbito militar como meio de partilha de informação segura. Expandiu-se através do hipertexto no âmbito militar, e é algo cíclico que a Guerra faz progredir a ciência e a tecnologia. O cyberspaço é uma evolução da internet, no sentido de aliar a tecnologia à sociedade surgindo então a sociedade de informação. Esta sociedade é constituída por pessoas, organizações, são empresas públicas ou privadas estando na base modelos de negócio.

- E-Governance, E-Cidadania, E-Policing, Conscencialização. A internet é vista como um espaço de liberdade e um vector de evolução, progresso e inovação.
- "O ciberespaço é o estado tecnológico mais aproximado da natureza humana." Está bem presente o dualismo entre o bem e o mal.
- "No ciberespaço circula informação e informação é poder. Este poder pode servir vários fins como por exemplo a ciberguerra"

Q2 – O que é e como é possível garantir a Cibersegurança das Infra-Estruturas Críticas Nacionais?

Conceito de Estratégia de defesa

- Vários eixos de actuação – Combate ao crime

Certificação e aplicação de normas internacionais para o uso das TIC

Protecção de infra-estruturas críticas

Acções de formação e consciencialização. Quer ao nível privado quer ao nível publico porque a cibersegurança é uma responsabilidade partilhada.

- Numa perspectiva reactiva tem de haver uma resposta a incidentes.

-Como os agentes criminosos nesta plataforma são extremamente inovadores, deverá haver um órgão de pesquisa e desenvolvimento nesta área tecnológica.

Relativamente às ECN

- Quem trabalha numa EC tem de ser consciencializado e tem que receber formação para poder adoptar condutas que salvaguardem os sistemas com que ele trabalha.

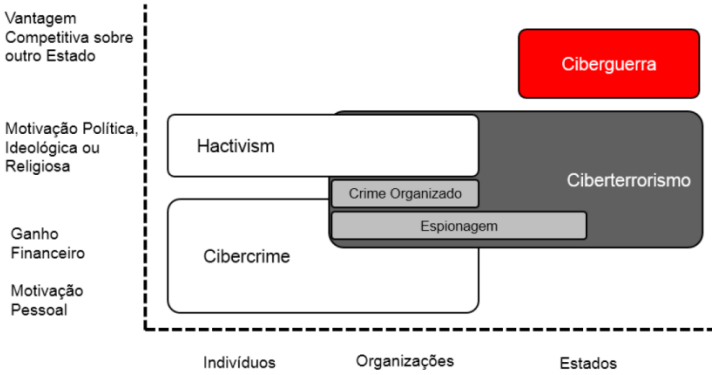
- Ao nível da governança. A hierarquia de topo deve estar consciencialização para esta nova realidade. E por vezes na Guarda não acontece pois estes perigos aparentemente não têm aparentemente materialização em danos à nossa estrutura.
- A meu ver isto deve-se devido a uma diferença geracional, em que as gerações anteriores não cresceram envolvidos nesta sociedade da informação e das novas tecnologias. Portanto eu prevejo que a Guarda encare este fenómeno com a sua devida importância quando se concretizar alguma destas ameaças mais graves e que haja consequências a nível interno.
- As gerações mais recentes já estão mais alertados e mais conscientes do perigo existentes no ciberespaço

RCM 12/2012

- Este conceito surge no âmbito da EU e porque os seus países constituintes estão extremamente alarmados para esta nova realidade

É fundamental haver um correcto funcionamento do aparelho legislativo nomeadamente na área do CP e CPP, não só a nível Internacional mas também a transição para o normativo nacional.
A prova digital é extremamente volátil. É necessário manter a custódia da prova.
Se os procedimentos previstos CPP para a preservação da prova não forem agilizados essa prova digital rapidamente se torna impossível se processar e analisar, não sendo possível traçar o percurso criminal do agente criminoso.

Q 3 – Qual é o espectro da ameaça no Ciberespaço e quais os principais desafios que coloca às Forças e Serviços de Segurança e à GNR em particular?



Q.4 – Qual o impacto das Ciberameaças na actividade da GNR?

- Relativamente os sistemas de informação da GNR são ferramentas de apoio e suporte à decisão e à actividade operacional, ou seja permitem a quem necessita, ter acesso à informação disponível mais rapidamente. Exemplo prático: a consulta de dados numa acção de fiscalização rodoviária que nos dias de hoje a consulta de alguma informação é praticamente imediata.

Diferença de «**Sistema informático»,** qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção; diferente de Sistema de informação é um ou um conjunto de sistemas informáticos que compila, trata, analisa a informação e apresenta-a de forma a facilitar e apoiar o processo de decisão. Como por exemplo o SIG – Sistema de Informação Geográfica - em que permite acompanhar em tempo real a localização das patrulhas no terreno e escolher qual a mais próxima de uma ocorrência.

Q.5 Que alterações ou ajustamentos serão necessários realizar na GNR para garantir uma maior eficácia de actuação no desempenho da sua missão em prol da Cibersegurança e da segurança das Estruturas Críticas Nacionais?

Existe já uma Unidade Curricular na Academia Militar

Agilização das medidas cautelares e de polícia.

As tecnologias da Informação são meios utilizados para cometer um grande espectro de ilicitudes, como por exemplo a violação de dados pessoais, violação de direitos de autor, pornografia infantil, etc

Devemos apostar em desenvolver competências na recolha de prova forense na área digital pois permite-nos agir fora do âmbito da Lei do Cibercrime. Considerando que as Leis estão em constante adaptação e tendo em conta a outros crimes foram despenalizados noutras, de forma a agilizar os processos jurídicos e os Tribunais, adquirindo estas competências as FFSS ou outras entidades administrativas. Neste cenário a Guarda é um potencial preencher este vazio de poder.

A aposta na formação poderá abrir portas no sentido de aquirir as competências necessárias para coadjuvar o poder político, órgãos ou entidades que tenham responsabilidades nesta área da segurança das IC, sendo que poderíamos participar na elaboração de planos emergência ou outras questões de segurança. Participando nestes projectos a Guarda estaria ciente das medidas adoptadas e mais facilmente poderia fazer cessar alguma ilicitude.

-A aposta num modelo policial nesta área que é o CyberPolicing que prima pela consciencialização das pessoas, empresas e outras entidades para estas questões da cibersegurança. Trabalhar numa perspectiva de aconselhamento, prevenção e consciencialização da responsabilidade partilhada que é a cibersegurança.
Em termos estratégicos estas iniciativas, como no âmbito da escola segura, a consciencialização das crianças para os riscos da Internet e as Redes Sociais, podem ser catapultadas para a criação de paradigmas de actuação face a estas novas ameaças.
Isto passa também pela iniciativa dos Órgãos de Topo e decisão, a definição de estratégias de acção para que os patamares de execução trabalhem esta área.
Aposta na criação e regulação de normas de segurança e boas práticas das ICI e sistemas e recursos informáticos

- Definição e padronização dos conceitos e doutrina para a Guarda e a nível nacional para que todos os elementos utilizem a mesma linguagem. Isto iria aproximar a Guarda de outras entidades externas como entidades públicas e privadas. Isto enquadrado como Cyberpolicing iria criar mais um nicho de actuação e especialização.
A nível internacional iria facilitar a cooperação ao nível da EU e da NATO. Havendo uma framework comum facilitará uma intervenção conjunta e padronizada ao nível internacional
Primar por explorar esta nova área e paradigma de intervenção policial ao nível das TIC o que poderia colocar a GNR numa posição privilegiada a nível das FFSS, constituindo-se como uma referência
- GNR mobile – nova iniciativa e consiste num sistema de Informações, Permite a disponibilização de informações em tempo real, o que permite a tomada de decisão em tempo útil. Funciona como uma sala de operações num telemóvel ou tablet.

- Propostas de constituição de uma Célula de cibersegurança (CSIRT) da GNR
Sob a alçada da Direcção de Informações ou sobre a alçada da Direcção de Comunicação e Sistemas de Informações.

Relatório Síntese da Entrevista ao Sr Major Pimentel

Q.1 – O que é o Ciberespaço e que desafios coloca às sociedades modernas e ao ambiente de Informação?

- Rede que interliga estes meios digitais, sejam eles servidores, computadores, telemóveis, tablets ou terminais de pagamento automático. Assenta numa rede que os dados digitais materializam transacções económicas ou sociais
- Desafios - Manter a segurança deste ciberespaço,
- Não há sistemas 100% seguros, o que se pode fazer é criar barreiras de protecção para salvaguardar a integridade deste sistema
- Desafio de encontrar o compromisso entre a segurança do sistema e a sua funcionalidade e custo.
- Não podemos criar um sistemas com tantas barreiras de segurança que o custo da criação dessas barreiras ultrapasse o custo da matéria a proteger

Barreira de Acesso físico (ex porta de Armas) Credenciação de password (no terminal)

Q2 – O que é e como é possível garantir a Cibersegurança das Infra-Estruturas Críticas Nacionais?

Dumper Diving e Engenharia Social

- A maior parte dos crimes que acontecem no Ciberespaço já aconteciam antes da existência deste meio, como por exemplo o roubo de Identidade ou documentos de identificação
- Falta um levantamento do conjunto de ECN de Informação e das suas necessidades específicas de segurança. Como por exemplo a transmissão de mensagens ou informações nas embaixadas Portuguesas
- CERT.pt
- Frameworks de segurança
- Oficialmente não há um levantamento das estruturas críticas da GNR, existe uma série de iniciativas que procuram promover boas práticas no que diz respeito à utilização de recursos informáticos.

O combate ao cibercrime tem de ser feito em três frentes.

1 A frente repressiva, em que é necessário capacitar os OPC para o travar e as autoridades criminais para o punir.

2 Formação das pessoas que estão ligadas ao aparelho judicial e policial

3 Formação e sensibilização e consciencialização da sociedade em geral

Ciberdefesa no contexto ofensivo/defensivo de Guerra

CISCO e CISSP – Framworks Cobit de segurança

Cibersegurança das ICI passa pelo levantamento das IC que tem activos informáticos a proteger.

Q 3 – Qual é o espectro da ameaça no Ciberespaço e quais os principais desafios que coloca às Forças e Serviços de Segurança e à GNR em particular?

A RNSI tem uma ferramenta que detecta os ataques feitos à rede e gera relatórios das ameaças ao sistema. Esta ferramenta só detecta os ataques que estejam sinalizados na base de dados da ferramenta como agentes maliciosos, ou seja ataques novos podem não ser detectados e nós não sabemos os seus efeitos a não ser através dos danos produzidos.

Q.4 – Qual o impacto das Ciberameaças na actividade da GNR?

Este impacto tem de ser medido a partir das potências ameaças e do levantamento dos mecanismos existentes para os proteger

Existe algum relatório

Levantamento dos activos críticos e quais os meios para os proteger.

Q.5 Que alterações ou ajustamentos serão necessários realizar na GNR para garantir uma maior eficácia de actuação no desempenho da sua missão em prol da Cibersegurança e da segurança das Estruturas Críticas Nacionais?

Levantamento dos activos críticos e quais os meios para os proteger. Processo de auditoria continua e supervisão.

Acções que levem a uma criação de uma Equipa de resposta a Incidentes e à criação de uma outra equipa de recolha de prova digital forense.

Esta equipa de recolha de prova digital forense deve estar certificada de forma a que toda a prova recolhida por esta seja válida em tribunal após ser analisada pela entidade competente.

A GNR pode actuar nesta área no que diz respeito às medidas cautelares e de polícia, sendo necessário que, no decorrer da actividade operacional, surja uma situação de necessidade ou oportunidade e de perca de prova.
A prova tem de ser certificada para a recolha dessa prova
Tem mantida a cadeia da custódia
Necessidade da criação
Pois a investigação dos crimes informáticos são da competência exclusiva da PJ.

Apêndice 1

Regulamento de Utilização dos Recursos Informáticos da GNR